TIPICO INFORMATION SECURITY GUIDELINES FOR SUPPLIERS

The Tipico Group (Tipico) is committed to high standards of Information Security and Data Privacy and has no tolerance policy when it comes to incompliant and malicious handling of all information relevant to the business and information of all natural persons and legal entities that maintain a business relationship with, and/or perform work for Tipico.

Tipico's Information Security Policy comprises the requirements that suppliers[1] must observer when accessing and using Tipico information and/or assets (e.g. IT devices and digital services) for processing said information, and/or when supplier information systems interact with Tipico information systems. If any requirements from the policy conflict with terms contained in any agreement between supplier and Tipico, the provisions providing greatest protection to the confidentiality, integrity, and availability of information prevail.

Tipico operates an Information Security Management System (ISMS) which complies with the requirements of the international standard ISO/IEC 27001:2013.

To guarantee the protection of information, assets, natural persons, and legal entities, supplier commits to comply with Tipico's Information Security Policy throughout the duration of the business relationship and to implement appropriate technical and organizational measures as required in the areas of:[2]

- Human resources security
- Physical security
- Access control
- Operations and communications security
- Risk management
- Information security and data privacy incident management
- Business continuity management
- Compliance

Third parties who have legitimate interest in accessing Tipico's ISMS documentation due to a business relationship, and desire to observe information security and data protection requirements in more detail, may obtain a copy of the Information Security Policy upon request.

---

[1] Suppliers are defined as any 3rd party that is providing services to Tipico based on a contractual relationship.

[2] Refer to Annex A for possible technical and organizational measures in the sub-sections of the respective area.

ANNEX A

The following is a non-exhaustive list of possible technical and organizational measures in the sub-sections of the main protection areas.

Human resources security	• Management support for staff prior, during, and through termination or change of employment • Relevant training and awareness
Physical security	• Centralized physical access management system, monitoring and surveillance • Appropriate protection measures for secure areas (e.g. server rooms and data centers) • Clear desk and clear screen
Access control	• Centralized identity and access management based on least privilege and need-to-know principles • Strong authentication and authorization • Information classification, auditing, and logging
Operations and communications security	• Technical security measures and controls to protect data in transit and at rest (e.g. encryption) • Active connectivity control and secure configuration requirements to minimize attack surface • Secure development lifecycle, change management, and vulnerability management
Risk management	• Risk based approach to data protection and security as emphasized by the GDPR • Effective risk-oriented decisions based on the severity and likelihood of risks
Information security and data privacy incident management	• Established security event detection and monitoring, response procedures, and reporting channels

	• Maintained logging, activity records, and audit trails • Security trainings, awareness campaigns, and continuous improvement processes
Business continuity management	• Appropriate mitigating measures to limit emergency events, crises, or disasters, including data breaches and cyber attacks • Established disaster response and recovery procedures • Backup plans and redundancies
Compliance	• Compliance with information security policies, industry regulations, and legal requirements

Document ID: L2.SP09.PI02 (V1.0_EN)

Target audience: All Tipico Suppliers

Classification: Limited public

Document history:

Version	Modifications	Date	Type	Author
0.9	Preview release	11.03.2022	Release	CISO
1.0	Release	05.05.2022	Release	CISO