Form

Information security guideline for suppliers

The importance of information security is constantly increasing. Confidentiality, integrity, availability and authenticity of values must be ensured in all processes. Thöni holds a TISAX label (VDA ISA catalogue) as a standard for information security. We work on the continuous improvement of our management system for information security and expect our suppliers to comply with the basic principles of information security. This includes, but is not limited to, the following points:

Information security organization
The company defines and lives policies, processes and responsibilities that guarantee, control and improve information security.

Assessment of the need for protection
All information security assets, information and processing systems of the company are defined, the need for protection in terms of confidentiality, integrity and availability is assessed and appropriate measures are derived. The measures are regularly reviewed for effectiveness.

Confidentiality and data protection
When exchanging confidential information between companies, appropriate confidentiality and data protection measures are guaranteed.

Legal Compliance
All relevant laws and guidelines relating to information security are complied with. They are regularly checked for updates and the internal processes based on them are adapted if necessary.

Access control and cryptography
Methods for user authentication (e.g., password, 2-factor authentication) are defined and implemented. Authorization concepts for information, systems and applications requiring protection have been defined. Suitable measures for encrypting personal information or information requiring protection are defined, documented and regularly checked concerning updates and security.

Physical and environmental safety
On the company's own premises, access to security-relevant information and equipment is only possible for authorized persons. Security zones have been defined for the company premises and suitable measures implemented to protect the information.

Privacy
Compliance with laws, regulations and possible contractual provisions on data protection guarantees that personal, sensitive data is secure at all times. Should data protection violations or incidents occur, they are immediately reported by phone (+43 5262 69 030) and in writing (compliance@thoeni.com) to Thöni In- dustriebetriebe, including details of the emergency plans.

Supplier relationships
The information security requirements are passed on to sub-suppliers and companies. Thöni will be informed immediately by phone (+43 5262 69 030) and in writing (compliance@thoeni.com) in case of inci- dents at sub-suppliers and sub companies .

Back-ups
Data requiring protection must be protected against destruction, loss and unauthorized access or modification. This is done, among other things, by creating a data backup concept, performing the data backups, and securely storing the data backups separately from the productive systems.

Protection against Malware
Technical vulnerabilities are protected by appropriate technical measures, such as virus protection programs, patch management and ongoing information on currently known attack scenarios.

Logging
The entry, modification and removal of data in IT systems are monitored. This includes logging the assignment of authorizations, checking user authorizations, and evaluating user and system activities.

Network security
Network management is in place, strong user authentication is in place for external connections and connections between individual systems, security gateways are used, diagnostic and configuration ports are protected, and sensitive systems are isolated.

Awareness
Regular training sessions on possible attack scenarios, personal options for defending against attacks, and the handling of sensitive data in the company are conducted and reviewed for effectiveness.

Behavior in case of an information security incident
Any disruptions relating to information security (e.g. malware, ransomware, phishing attacks) must be reported by phone (+43 5262 69 030) and in writing (compliance@thoeni.com) to Thöni Industriebetriebe within 24 hours Legal measures are communicated and documented.

Business Continuity Management
Contingency plans are in place to ensure continued operation in the event that valuable information is compromised by an attack. Critical components are redundant, and emergency measures are regularly checked for effectiveness.

Assessment and improvement
The effectiveness of the above-mentioned measures is reviewed on a regular basis. Registered weak points are closed in order to continuously improve the system as a whole. System checks can also be conducted by Thöni at the supplier's or service provider's premises. In this case the supplier or service provider cooperates fully and provides all necessary documents.