The company SLUŽBA NITRA, s. r. o. focuses on its own development and production of components for the automotive and electrotechnical industry. It is a supplier of TIER 1 for the most demanding customers VW GROUP, ŠKODA AUTO, AUDI, STELLANTIS, FORD, SEAT and for TIER 2 customers APTIV, FUJIKURA, SUMITOMO, KIEKERT, PLASIC OMNIUM LIGHTING, SMR, FICOMIRRORS, MAGNA and others.

Employees of SLUŽBA NITRA, s. r. o. do not agree with any forms of violence in international relations. No one may impose his demands by armed intervention.
Our security solution proposals are based on qualified risk analysis and classification of information assets. The biggest threat today is cyber-attacks and the spread of hoaxes. We regularly evaluate the risks that have arisen.
The priority is to protect the interests of the customer and the interested environment. We protect prototypes during design, testing, storage and logistics, including physical as well as data objects, against misuse or theft of related confidential data. We achieve our business goals without violating legal, customer, regulatory and contractual security requirements.
We take active measures to prevent unauthorized intrusion into the company's premises, so as not to destroy, damage, compromise the premises or information assets. We manage a logical approach to processed information using the "need to know" principle. We pay attention to achieving adequate protection of key information assets.
We ensure the correct and safe operation of means processing information. We comply with the requirements of laws and customer requirements to ensure cybersecurity.
We prevent interruptions in the supply of IT services.
We protect all information systems and networks so that business continuity is not compromised due to an accident or failure of information systems.
We ensure smooth restoration of obsolete or crashed systems to prevent financial losses and possible loss of reputation.
We monitor the environment, record and treat suspicious events, security incidents and purposefully prevent their recurrence.
Already when defining requirements, we define the requirements for knowledge of the applied Information Security Management System (SRIB). For each applicant or employee, we gather knowledge and plan additional training in the field of SRIB. We will not allow a worker who has had or has difficulty complying with confidentiality requirements. We monitor security incidents and identify whether undesirable activities of employees were not the cause of violation of the company's principles for Information and/or Cybersecurity. Workers are the most important source of our strength and success. Their qualifications, skills, involvement and satisfaction is a guarantee of the success of the company. We train our own employees, contractors and so-called third parties to understand their rights and obligations regarding the information security management system and the protection of prototypes against breach or theft of confidential data. We monitor and evaluate the achieved level of education.

In Nitra on 2024-01-15

Mgr. Martina Štefanková
Executive Manager

Ing. Miroslav Fülöp
CEO