Constellium

INFORMATION SECURITY POLICY

Company Constellium Extrusions Děčín s.r.o. including detached workplaces is aware of its responsibility to all stakeholders and therefore announces its Information Security Policy

Management commitment

Management of Constellium Extrusions Děčín s.r.o. (further as „DEC“) commits to support the implementation and operation of the Information Security Management System (further as "ISMS") by setting the Organization's Information Security Policy, setting ISMS objectives and a plan to achieve them, setting roles, duties and responsibilities in the field of information security, promoting the importance of meeting security objectives within the organization, providing the necessary resources, setting criteria for risk acceptance and accepted level of risk, ensuring internal ISMS audits and conducting ISMS reviews by the organization management.

Basic characteristic of information security

Information security is characterized as maintaining confidentiality, integrity and availability of information, whereby:

a. Confidentiality is an assurance, that information is not available or disclosed to unauthorized individuals, entities or processes,
b. Integrity means ensuring the accuracy and completeness of information and methods of its processing,
c. availability is an assurance that information is accessible and usable at request of an authorized individual, entity or process

Objectives and importance of information security in organization

The purpose of ISMS in DEC is to ensure the availability of information assets only to authorized persons, the accuracy and completeness of information, confidentiality and security of their processing and protection of information against accidental or unauthorized destruction or accidental loss, unauthorized access, alteration or dissemination, in accordance with laws and other legal regulations of the Czech Republic.

Organization security strategy

The information security management system is implemented in accordance with the ČSN ISO / IEC 27001: 2014 standard and within the scope of implementation of measures according to Annex A of this standard, depending on the results of the risk assessment.

Basic definition of responsibilities

The organization's management defines functions to which the relevant roles, responsibilities and authorities for information security management are assigned.

Information Security Management Committee (further as „Committee“) - consists of persons with relevant competences and professional qualifications for the overall management and development of ISMS and persons significantly involved in the management and coordination of activities related to information security. Member of the committee must always be at least one representative of the organization's senior management or a person authorized by management and the Information Security Manager. In the case of Constellium, the powers of the committee shall be held by a meeting of the company's management.

Information Security Manager – is subordinate to the organization´s management. Implements the security principles of the organization's Information Security Policy and proposes its changes, monitors compliance with security measures and the implementation of their changes, ensures risk assessment, resolution of security incidents and raising the security awareness of the organization's employees.

Asset guarantee - is a security role responsible for defining the requirements for the development, use and security of a primary or supporting asset.

Information Security Auditor - an employee who is designated as the organization's internal ISMS auditor.

Risk assessment and information security requirements

Assets are evaluated for confidentiality, availability and integrity. The risk assessment is performed on the basis of risk identification, analysis and assessment and aims to identify possible threats, vulnerabilities and risks of the assessed system, to estimate losses that may arise due to threats to information assets included in the organization's ISMS. Safety measures (Declaration of Applicability, Risk Management Plan) are taken to cover the identified risks, to prevent or reduce adverse effects and to achieve continuous improvement. Risk assessments and asset evaluations are performed on a regular basis every three years or in the event of major changes in the assessed area.

Training and education requirement

The organization shall ensure that the staff covered by the duties defined in the ISMS are professionally qualified to perform the required tasks. Qualification is maintained by training or education according to professions, at intervals specified in applicable regulations.

Internal audit

To ensure protection of the operated information systems and the ISMS system, a regular information security audit is performed. Audit requirements and activities involving the control of the organization's ISMS are planned by the Information Security Auditor and approved by the company's management at least once a year.

Regular review

The review of the information security management system is performed in order to ensure the usefulness, adequacy and effectiveness of the ISMS operated in the organization. The ISMS review also identifies opportunities for improvement and proposes changes to the ISMS it operates. The ISMS review interval in DEC is set to once a year.

Indication of consequences in case of non-compliance with the policy

All employees are aware of the fact that non-compliance with safety principles can be qualified as a breach of employee duties and in some cases as an offense or a crime.

Revision

The information security policy is available to all employees on the corporate intranet and to external partners on the company's website. The security policy is revised by its owner at least once a year or in the event of a significant change affecting its timeliness and validity. The date of issue of the valid revision is expressed by the date of issue of the security policy.

Follow-up documentation

The Information Security Policy is followed by ISMS documentation developing measures for information security. These documents contain specific responsibilities for the implementation of information security processes and activities.

The hierarchy of ISMS documentation in DEC is as follows:

1. Information security policy (this policy),
2. Information Security Directive and User Security Directive
3. Records for ISMS support (in particular risk assessment documentation, security zone documentation, supplier-related documentation, security incident records, business continuity plan, ISMS internal audit documentation, non-compliance records and regular review of information security status).

The management of ISMS documentation is described in org. directives ISŘ-22 and VS-09.

Jiří Palma	Miloslav Šoltys	Jan Bibík	Libor Voborský	Jan Šípal
Managing Director	Technical Director	Production Director	Sales Director	Finance Director

February 1st 2024