KOLEKTOR

Politika upravljanja in varovanja informacij

V skupini Kolektor se zavedamo, da imajo informacije za nas ključno vrednost, zato imamo za njihovo zaupnost, celovitost in razpoložljivost vzpostavljen Sistem upravljanja in varovanja informacij (SUVI), ki je integriran v sistem vodenja družbe.

S sistemom SUVI sistematično in celovito pristopamo k varovanju informacij, informacijskih sredstev in virov, preprečujemo neželene informacijske varnostne dogodke ter zmanjšujemo posledice in potencialno škodo, skladno s priporočili standarda ISO/IEC 27001.

SUVI obsega:

- zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij,
- varovanje informacij pred nepooblaščenimi dostopi, razkritjem, spremembami ali uničenjem,
- ozaveščanje in izvajanje usposabljanja o informacijski varnosti,
- seznanjanje s pravili varne uporabe informacijske infrastrukture,
- obvladovanje varnostnih incidentov ter pravočasno in ustrezno ukrepanje,
- redno analiziranje tveganj in njihovo zmanjševanje.

V vse procese sistematično uvajamo ukrepe, katerih namen je izboljšati stopnjo zaupnosti informacij, zmanjšati možnost pojava nerazpoložljivosti informacij, povečati stopnjo celovitosti in avtentičnosti informacij ter s tem zagotoviti kontinuirano poslovanje.

Tako zaposleni kot poslovni partnerji smo s svojim ravnanjem dolžni vsak zase prispevati k informacijski varnosti in nenehnemu izboljševanju sistema SUVI, saj nam doba digitalizacije predstavlja še večjo izpostavljenost varnostnim grožnjam in odtekanjem informacij iz poslovnega okolja.

Valter Leban
Predsednik uprave
Skupine Kolektor

KOLEKTOR

Information Security Policy

In Kolektor, we are aware that information is of key value to us, therefore, we have established the Information Security Management System (ISMS) to keep confidentiality, integrity and availability of such information. ISMS is integrated into the company's management system.

With the ISMS, we systematically and comprehensively approach the protection of information, information assets and resources, prevent unwanted information security events, and reduce the consequences and potential damage, in accordance with the recommendations of the ISO / IEC 27001 standard.

ISMS includes:

- ensuring the confidentiality, integrity and availability of information,
- protecting information from unauthorized access, disclosure, alteration or destruction,
- raising awareness and providing training on information security,
- getting acquainted with the rules of safe use of information infrastructure,
- managing all security incidents and taking timely and appropriate actions,
- regulary analyzing risks and reducing them with appropriate measures.

We systematically introduce measures into all processes in order to improve the level of confidentiality of information in Kolektor, reduce the possibility of unavailability of information, increase the level of integrity and authenticity of information and thus ensure continuous operation.

Both employees and business partners are obliged to contribute to information security and the continuous improvement of the ISMS, as the digital age represents an even greater exposure to security threats and information leakage from the business environment.

Valter Leban
President of the Management
Board of Kolektor