



Kybernetická bezpečnosť Politika

Siemens Regional Country Slovakia

Kybernetická bezpečnosť (CYS) je dôležitou otázkou pre budúcnosť - pre firmy aj spoločnosť. Je kľúčovým predpokladom pre organizácie na ochranu kritickej infraštruktúry, ochranu citlivých informácií a zabezpečenie kontinuity podnikania. Siemens berie túto zodpovednosť veľmi vážne a preto je spoluzakladateľom a aktívnym partnerom „Charty dôvery“ (<https://www.charteroftrust.com>).

Ciele kybernetickej bezpečnosti Siemens sú zabezpečiť IT/OT infraštruktúru (informačné technológie / operačné technológie), zabezpečiť informačnú bezpečnosť počas celého životného cyklu produktov, riešení a služieb Siemens, ako aj vo všetkých interných obchodných procesoch.

Kybernetická bezpečnosť ovplyvňuje a je ovplyvňovaná každým zamestnancom spoločnosti Siemens. V dôsledku toho je kybernetická bezpečnosť spoločnou úlohou, kde stupeň zapojenia a zodpovednosti závisí od jednotlivých rolí a funkcií.

Sme odhodlaní plniť si svoju zodpovednosť v tomto ohľade.

Toto je zabezpečené nasledujúcimi zásadami:

- Dodržiavanie externých právnych predpisov a špecifikácií hlavných štandardov kybernetickej bezpečnosti, ako sú ISO 27001 a TISAX, ako aj dodržiavanie interných celopodnikových predpisov kybernetickej bezpečnosti.
- Definícia organizačnej štruktúry s jasnými zodpovednosťami a merateľnými cieľmi kybernetickej bezpečnosti
- Poskytovanie primeraných zdrojov na plánovanie, implementáciu, monitorovanie a neustále zlepšovanie prevádzkovej efektívnosti ISMS (systému riadenia informačnej bezpečnosti)
- Ponuka interných komunikácií a školení na neustále podporovanie vhodného správania všetkých zamestnancov
- Posilňovanie odolnosti na zabezpečenie optimálnej kontinuity podnikania (BCM)
- Implementácia kybernetickej bezpečnosti ako neoddeliteľnej súčasť obchodnej stratégie

Pre našu spoločnosť, zákazníkov a Siemens sme dôveryhodným partnerom - v reálnom aj digitálnom svete.

Vladimír Slezák
Chief Executive Officer

Pavel Lakatos
Chief Financial Officer



Prosím, navštívte našu webovú stránku, kde nájdete informácie o riadení kybernetickej bezpečnosti:



Cybersecurity Policy

Siemens Regional Country Slovakia

Cybersecurity (CYS) is an important issue for the future – for companies and society. It is a key prerequisite for organizations to safeguard critical infrastructure, protect sensitive information and assure business continuity. Siemens takes this responsibility very seriously and is therefore a co-founder and active partner of the „Charter of Trust“ (<https://www.charteroftrust.com>).

The objectives of Cybersecurity at Siemens are to secure the IT/OT infrastructure (Information Technology / Operational Technology), to ensure information security along the lifecycle of Siemens products, solutions and services, as well as in all internal business processes.

Cybersecurity affects and is affected by every employee of Siemens. Consequently, Cybersecurity is a collaborative task where the degree of involvement and responsibility depends on the individual roles and functions.

We are committed to fulfilling our responsibility in this regard.
This is ensured by the following principles:

- Compliance with external legal regulations and specifications of major cybersecurity standards such as ISO 27001 and TISAX, as well as adherence to internal company-wide cybersecurity regulations.
- Definition of an organizational structure with clear responsibilities and measurable cybersecurity objectives.
- Offering internal communications and training to continuously promote appropriate behavior among all employees.
- Strengthening resilience to ensure optimal business continuity (BCM).
- Implementing cybersecurity as an integral part of the business strategy.

For our society, customers and Siemens, we are a trusted partner – both in the real and the digital world.

Vladimír Slezák
Chief Executive Officer

Pavel Lakatos
Chief Financial Officer



Please visit our website to get further information about Cybersecurity Governance: