

## Információbiztonsági Politika

Siemens Zrt.

Az információbiztonság igen fontos feladat a jövőre nézve – úgy a vállalatok, mint a társadalom számára is. Kulcsfontosságú előfeltétel a szervezeteknek, hogy megvédjék kritikus infrastruktúrájukat, érzékeny adataikat és biztosíthassák üzletmenetük folytonosságát. A Siemens komolyan veszi ezt a felelősség-vállalást, éppen ezért társalapítója és aktív partnere a „Charter of Trust” szervezetének. (<https://www.charteroftrust.com>).

Jelen információbiztonsági politika célja magas szinten támogatni és szabályozni a Siemens Zrt. alapfeladatainak zavartalan ellátásához szükséges adatvédelmi és információbiztonsági alapelveket.

Célunk továbbá, hogy megvédjük az IT/OT infrastruktúrát (Information Technology / Operational Technology), biztosítsuk az információbiztonságot a Siemens termékek, megoldások és szolgáltatások életciklusának folyamán csakúgy, mint a belső üzleti folyamatokban.

A politika hatálya kiterjed a vállalat valamennyi folyamatára és szervezeti egységére, így különösen az elektronikus információs rendszereire, mely magában foglalja az adathordozókat, alkalmazásokat, szoftvereket, hardver elemeket, a környezeti infrastruktúra elemeit és objektumait, a papír alapú dokumentumokat, továbbá minden eljárásra, melyek hatással lehetnek a Siemens adatvagyonára.

Az információbiztonság és minden egyes Siemens munkavállaló kölcsönösen hatással van egymásra, melynek során a felelősség-vállalás és részvétel mértéke az egyéni szerepektől és funkcióktól függ.

Elkötelezettek vagyunk abban, hogy fentiek vonatkozásában felelősséget vállaljunk, a következő alapelvek mentén:

- megfelelés a főbb jogi és egyéb külső előírásoknak, szabványoknak, mint például ISO 27001, TISAX, valamint a belső, vállalati szintű információbiztonsági szabályozásoknak,
- szervezeti hierarchia kialakítása az információbiztonság szempontjából egyértelmű felelősségi körökkel és mérhető célokkal,
- megfelelő erőforrás biztosítása az ISMS (Information Security Management System) rendszer működési hatékonyságához szükséges tervezési, implementációs, ellenőrző és folyamatos fejlesztési tevékenységekhez,
- belső kommunikáció és oktatás biztosítása a szükséges munkavállalói magatartás folyamatos támogatásának érdekében,
- rugalmasságunk erősítése az optimális üzleti folytonosság érdekében,
- az információvédelem bevezetése az üzleti stratégia integráns részeként.

Vezetésünk a politikában megfogalmazott elvek és követelmények teljesítését várja el cégünk összes munkatársától, szállítótól és minden egyéb érdekelt féltől.

**Társadalmunk és üzleti partnereink számára a Siemens megbízható partner – mind a valós mind pedig a digitális világban.**

Budapest, 2022. május 2.

Jeránek Tamás  
Elnök-vezérigazgató

Károlyi Zsolt  
Gazdasági Igazgató



## Cybersecurity Policy

### Siemens Hungary

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 legislation and the specifications of major Cybersecurity standards like ISO 27001, ISO 62443 or TISAX as well as adherence to internal company-wide Cybersecurity regulations
- Definition of an organizational structure with clear responsibilities and measurable objectives of Cybersecurity
- Provision of adequate resources to plan, implement, monitor as well as continuously improve the operational effectiveness of the ISMS (Information security management system)
- Offer of internal communications and training to continuously promote appropriate behavior of all employees
- Strengthening of resilience to ensure optimal Business Continuity (BCM)
- Implementation of Cybersecurity is 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.**

Budapest, 2nd May 2022

Tamás Jeránek  
CEO

Zsolt Károlyi  
CFO

