

## Politika bezpečnosti informací a majetku

Skanska v České a Slovenské republice je člen mezinárodního koncernu Skanska a řadí se k největším stavebním firmám působícím na stavebním trhu v České a Slovenské republice.

Naší snahou je zajistit kontinuitu podnikatelské činnosti skupiny, minimalizovat případné škody předcházením bezpečnostním incidentům a deklarovat našim zákazníkům, obchodním partnerům, akcionářům, zaměstnancům a široké veřejnosti schopnost skupiny efektivně ochránit informace a majetek vlastní i svěřený v souladu s relevantními závaznými právními normami a požadavky zemí, ve kterých skupina podniká, a s požadavky mateřské společnosti Skanska Kraft AB.

K prosazení této politiky jsou ve skupině jako neoddělitelné součásti řízení zavedeny a udržovány ISMS - systém řízení informační bezpečnosti podle ČSN ISO/IEC 27001 a systém opatření zajišťujících připravenost skupiny k realizaci zakázek s požadavkem na ochranu utajovaných informací podle právních norem zemí, ve kterých skupina působí.

Deklarujeme, že:

- Jsou naplněny všechny požadavky relevantních právních předpisů, které jsou na skupinu kladeny v oblasti bezpečnosti informací a majetku.
- Informace jsou dostupné kdykoli a kdekoli pro potřeby businessu.
- Informace jsou vždy správné a pravdivé. Informace přečtená z nosiče je stejná jako byla v okamžiku, kdy byla na nosič zapsána. Je zajištěno řízení celého životního cyklu informací, tzn. jejich zpracování od okamžiku získání nebo vytvoření až po jejich předání nebo likvidaci.
- Informace jsou zpřístupněny jen tomu, kdo je potřebuje pro účely businessu - princip „need-to-know“. Je minimalizován únik informací v případě odchodu zaměstnanců.
- Zaměstnanci jsou trvale vzděláváni a školeni v oblasti bezpečnosti informací.
- Porušení pravidel bezpečnosti informací je považováno za hrubé porušení interních předpisů a pracovních povinností a je postihováno v souladu se zákoníkem práce.
- Přijímaná bezpečnostní opatření jsou přímo úměrná aktuální míře rizik.
- Pravidelným monitorováním, hodnocením rizik, řízením bezpečnostních událostí a incidentů nápravných a preventivních opatření budeme zvyšovat účinnost systému řízení bezpečnosti informací a majetku.

Politika bezpečnosti informací a majetku je závazná pro všechny zaměstnance skupiny Skanska v ČR a SR

Vedení společnosti Skanska trvale prověřuje efektivnost svých činností při naplňování této politiky pravidelným vyhodnocováním a svými plány se snaží maximálně naplnit tuto politiku.



Ing. Dan Ťok  
generální ředitel a předseda představenstva

## Policy of Information Security and Asset Security

The Skanska companies in the Czech Republic and Slovakia are part of the multinational Skanska Group and are collectively one of the largest construction companies operating on the Czech and Slovak markets.

Our approach is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents. Also, to affirm to our customers, business partners, shareholders, employees and general public our ability to efficiently protect the information and assets. Lastly, to ensure we are compliant with regulatory and legislative requirements of countries where Skanska group operates and with demands of parent corporation Skanska Kraft AB.

Information Security Management System (ISMS – according to international standard ISO/IEC 27001) and system of controls for protection of classified information on local country level (compliant with local countries, EU and NATO) are implemented to enforce this policy.

We declare:

- We achieved all demands of obligatory rules of law which are set in the area of information security and assets for our group.
- Information is available whenever and wherever business needs it.
- Information is always accurate and truthful. Information read from media is equal to the information originally on media recorded. All the lifecycle of the information is controlled from its obtaining or creating to its handing over or deleting.
- Information is available only for those who need it for the purpose of business – principle “need-to-know”. Information leakage in case of staff leaving the company is minimized.
- Staff is constantly trained and educated in the area of Information Security.
- Violation of information security rules would be considered for rude violence of Skanska internal regulations and labor service and would be punished in compliance with Labor Code.
- Implemented security controls adequately correspond to the level of the risks.
- We will improve the efficiency of information security & assets system via regular monitoring, risk evaluation, control of security incidents and preventive steps.

This Policy of Information Security and Assets Security is mandatory for all Skanska employees in the Czech Republic and Slovakia.

Skanska top management continuously checks the efficiency of implemented security controls by regular evaluation and makes effort to fulfill this policy through business planning.



Dan Ťok  
Chairman of Board of Directors and CEO