

## Politika bezpečnosti informácií a majetku

Skanska v Českej a Slovenskej republike je členom medzinárodného koncernu Skanska a radí sa k najväčším stavebným firmám pôsobiacim na stavebnom trhu v Českej a Slovenskej republike.

Našou snahou je zaistiť kontinuitu podnikateľskej činnosti skupiny, minimalizovať prípadné škody predchádzaním bezpečnostným incidentom a deklarovať naším zákazníkom, obchodným partnerom, akcionárom, zamestnancom a širokej verejnosti schopnosť skupiny efektívne chrániť informácie a majetok vlastný i zverený v súlade s relevantnými záväznými právnymi normami a požiadavkami štátov, v ktorých skupina podniká, a s požiadavkami materskej spoločnosti Skanska Kraft AB.

K presadeniu tejto politiky sú v skupine ako neoddeliteľné súčasť riadenia zavedené a udržiavané ISMS – systém riadenia informačnej bezpečnosti podľa ISO/IEC 27001 a systém opatrení zaisťujúcich pripravenosť skupiny k realizácii zákaziek s požiadavkou na ochranu utajovaných informácií podľa právnych noriem štátov, v ktorých skupina pôsobí.

Deklarujeme, že:

- Sú naplnené všetky požiadavky relevantných právnych predpisov, ktoré sú na skupinu kladené v oblasti bezpečnosti informácií a majetku.
- Informácie sú dostupné kedykoľvek a kdekoľvek pre potreby businessu.
- Informácie sú vždy správne a pravdivé. Informácia prečítaná z nosiča je rovnaká ako bola v okamžiku, keď bolo na nosič zapísaná. Je zaistené riadenie celého životného cyklu informácií, t.z. ich spracovania od okamžiku získania alebo vytvorenia až po ich odovzdanie alebo likvidáciu.
- Informácie sú prístupné len tomu, kto ich potrebuje pre účely businessu – princíp „need-to-know“. Je minimalizovaný únik informácií v prípade odchodu zamestnancov.
- Zamestnanci sú trvale vzdelávaní a školení v oblasti bezpečnosti informácií.
- Porušenie pravidiel bezpečnosti informácií je považované za hrubé porušenie interných predpisov a pracovných povinností a je postihované v súlade so zákonníkom práce.
- Prijímané bezpečnostné opatrenia sú priamo úmerné aktuálnej miere rizík.
- Pravidelným monitorovaním, hodnotením rizík, riadením bezpečnostných udalostí a incidentov nápravných a preventívnych opatrení budeme zvyšovať účinnosť systému riadenia bezpečnosti informácií a majetku.

Politika bezpečnosti informácií a majetku je záväzná pre všetkých zamestnancov skupiny Skanska v ČR a SR.

Vedenie spoločnosti Skanska trvale preveruje efektívnosť svojich činností pri naplňovaní tejto politiky pravidelným vyhodnocovaním a svojimi plánmi sa snaží maximálne naplniť túto politiku.



Ing. Dan Ťok  
generálny riaditeľ a predseda predstavenstva

## 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