Závazek kyberbezpečnosti TSC GROUP, a.s. a jednotlivých dceřiných společností

Bezpečnost informací a ochrana dat je pro koncern TSC GROUP, a.s. a jeho jednotlivé dceřiné společnosti, strategickou prioritou. V době, kdy digitální technologie a online komunikace tvoří základ našich interních procesů i služeb poskytovaných zákazníků, je pro nás zásadní zajistit důvěrnost, integritu a dostupnost všech informací. Tento dokument shrnuje náš závazek k bezpečnému a odpovědnému nakládání s daty a informačními systémy, a to v souladu s mezinárodními normami a legislativními požadavky, včetně ISO/IEC 27001 a směrnice NIS II.

Principy a závazky

1. **Ochrana dat** – Chráníme data zákazníků, zaměstnanců, naše know-how i interní informace před ztrátou, zneužitím nebo neoprávněným přístupem.
2. **Řízení rizik** – Systematicky identifikujeme, hodnotíme a minimalizujeme informační a kybernetická rizika.
3. **Transparentní a odpovědné řízení** – Zavádíme jasné procesy, pravidelné audity a monitorování bezpečnosti, abychom zajistili efektivní kontrolu a soulad s legislativou a interními pravidly.
4. **Vzdělávání a povědomí zaměstnanců** – Každý zaměstnanec každé dceřiné společnosti v koncernu TSC GROUP, a.s. je pravidelně školen v oblasti kyberhygieny, bezpečného používání systémů a postupů pro prevenci incidentů.
5. **Technická a organizační opatření** – Implementujeme víceúrovňová bezpečnostní opatření, včetně firewallů, šifrování, přístupových oprávnění a monitorovacích systémů, aby byla zajištěna odolnost IT infrastruktury.

Certifikace a standardy

V roce 2026 budou jednotlivé společnosti v koncernu TSC GROUP, a.s. certifikovány podle ISO/IEC 27001, což potvrzuje zavedení systému řízení bezpečnosti informací podle mezinárodních standardů. Současně naše systémy a procesy podléhají požadavkům směrnice NIS II, která stanovuje povinnosti týkající se kybernetické bezpečnosti v rámci kritické infrastruktury a digitálních služeb.

Prevence a reakce na incidenty

- V případě kybernetických incidentů máme zavedeny jasné postupy pro jejich rychlou identifikaci, řešení a minimalizaci dopadů.
- Pravidelně provádíme testování zranitelností, penetrační bezpečnostní testy a simulace incidentů pro ověření odolnosti našich systémů.
- Vytváříme plán obnovy po incidentu a kontinuální monitorování IT infrastruktury, aby byla zajištěna nepřetržitá dostupnost klíčových služeb.

Role zaměstnanců

Bezpečnost informací je odpovědností každého z nás. Zaměstnanci jednotlivých dceřiných společností v koncernu TSC GROUP, a.s. se podílejí na ochraně dat tím, že:

- dodržují interní bezpečnostní předpisy,
- používají bezpečné přihlašovací údaje a systémy autentizace,

TSC GROUP, a.s.
Stodolní 316/2, 702 00 Ostrava – Moravská Ostrava
IČ: 294 52 066 · DIČ: CZ29452066
t: +420 605 223 375, e: info@tsc-group.cz
www.tsc-group.cz

B 10331 vedená u Krajského soudu v Ostravě.

- hlásí podezřelé aktivity a incidenty,
- aktivně se účastní školení a zvyšují své povědomí o kybernetických hrozbách.

Cíle pro rok 2026

1. Zavést certifikovaný systém řízení bezpečnosti informací podle ISO/IEC 27001.
2. Plnit požadavky NIS II a zajistit soulady s právními předpisy.
3. Posílit kybernetickou ochranu a víceúrovňová bezpečnostní opatření.
4. Pravidelně školit zaměstnance a zvyšovat jejich povědomí o bezpečnosti informací.
5. Implementovat efektivní monitoring, prevenci a plán reakce na incidenty.

TSC GROUP, a.s., jakož i její dceřiné společnosti, se zavazují, že kyberbezpečnost bude neustále prioritou ve všech procesech, projektech i v každodenní činnosti, a že každý zaměstnanec kterékoliv ze společností v koncernu TSC GROUP, a.s. přispěje k ochraně informací, spokojenosti zákazníků a dlouhodobé důvěryhodnosti společnosti.

V Ostravě 2.1.2026

TSC GROUP, a.s.
Radek Fál, Mgr. Robert Labuda
představenstvo společnosti

TSC GROUP, a.s.
Stodolní 316/2, 702 00 Ostrava – Moravská Ostrava
IČ: 294 52 066 · DIČ: CZ29452066
t: +420 605 223 375, e: info@tsc-group.cz
www.tsc-group.cz

B 10331 vedená u Krajského soudu v Ostravě.