Bezpečnostní politika DPMB, a.s.

Bezpečnostní politika Dopravního podniku města Brna, a.s. (dále jen DPMB, a.s.) definuje základní strategii a zásady týkající se managementu zabezpečení informací (ISMS) v souladu s ČSN EN ISO/IEC 27001:2023. Určuje základní bezpečnostní pravidla pro provoz, používání a údržbu informačních a komunikačních technologií s cílem zajistit požadovanou dostupnost a ochranu informací a minimalizaci možných škod vzniklých v důsledku možných bezpečnostních incidentů.

Prohlášení managementu

Vizí DPMB, a.s. je zvyšování kvality MHD, udržení pozice DPMB, a.s. v rámci Integrovaného dopravního systému Jihomoravského kraje a nabídka pro veřejnost přitažlivé hromadné dopravy na úrovni Evropské unie. Bezpečnost zpracovávaných informací je vedením DPMB, a.s. chápána jako důležitý nástroj, podporující dosahování této vize.

Vedení DPMB, a.s. si je vědomo nezbytnosti a prospěšnosti péče o bezpečnost. Systematicky podporuje procesy využívání a rozvoje ISMS. Pro zajišťování dosahování požadované úrovně bezpečnosti se vytyčují cíle, které jsou pravidelně vyhodnocovány.

Bezpečnostní povědomí zaměstnanců je u DPMB, a.s. soustavně upevňováno. Povinnosti a pravidla jsou pravidelně školeny.

Rozsah ISMS a účinnost opatření k zajištění bezpečnosti jsou v rámci soustavného zlepšování systému pravidelně přezkoumávány v rámci přezkoumání systému managementem společnosti.

V souladu s požadavky ČSN EN ISO/IEC 27001:2023 vyhlásilo vedení společnosti Bezpečnostní politiku DPMB, a.s. jako svůj závazek. Záměrem vedení je podporovat cíle a principy bezpečnosti informací.

Hlavní zásady práce s informacemi a způsob jejich zabezpečení:

- zajistit odpovídající ochranu osobních údajů v souladu s platnou legislativou,
- vytvářet a prosazovat systém řízeného přístupu k informacím,
- začleňovat zabezpečení informací do odpovědnosti za práci,
- zajišťovat systematické vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací,
- provádět stálou identifikaci bezpečnostních incidentů a přijímat účinná opatření pro zlepšování bezpečnosti informací,
- zpracovávat soubory opatření pro zachování kontinuity pro případy závažného výpadku v oblasti informací, tato opatření pravidelně přezkušovat a ověřovat,
- zabezpečovat informační systémy, internet, elektronickou poštu a další způsoby výměny informací přístupných veřejnosti,

- zabezpečovat systém fyzického přístupu do prostor pro snížení ohrožení informačního majetku,
- prosazovat politiku bezpečného pracoviště: čistý stůl, prázdné obrazovky a odpadkové koše,
- prosazovat bezpečnostní pravidla pro přenosná počítačová zařízení a jiné nosiče informací,
- zajišťovat spolehlivou kontrolu celé interní sítě proti působení škodlivého softwaru,
- udržovat, chránit a rozvíjet informační majetky, spolehlivě zálohovat informační systémy,
- pravidelně monitorovat a vyhodnocovat bezpečnostní rizika a incidenty,
- zabezpečit požadavky vyplývající ze smluvních závazků a obecně závazných právních předpisů,
- zabezpečit včasnou dostupnost informací – doba kritické dostupnosti informací musí být stanovena, a to v souladu s jejich významem,
- zamezit nežádoucí modifikaci informací,
- zamezit zneužití nebo ztráty informací, musí být definována odpovědnost a způsob ochrany při přístupu k informacím a do prostor kde se nachází informační majetky,
- provádět stálou identifikaci bezpečnostních incidentů a přijímat účinná opatření pro zlepšování bezpečnosti informací; pravidelně monitorovat a vyhodnocovat bezpečnostní rizika
- analyzovat příčiny porušení pravidel a přijímat účinná opatření s cílem, aby se v budoucnu neopakovala.

Odpovědnost zaměstnanců

- každý zaměstnanec, kterému byl umožněn přístup k informačním prostředkům pro potřeby výkonu pracovní činnosti, přebírá odpovědnost za bezpečné nakládání s těmito prostředky a za ochranu informací ve své působnosti,
- politika bezpečnosti informací a související dokumentace je závazná pro všechny zaměstnance s přístupem k informacím, a to bez ohledu na zastávanou funkci, pozici či roli ve společnosti. Všichni zaměstnanci nesou v souladu s platnou legislativou a předpisy svůj díl zodpovědnosti za dodržení, resp. porušení pravidel, s nimiž byli seznámeni. Všichni zaměstnanci jsou povinni předepsaným způsobem reagovat na závady, poruchy a bezpečnostní incidenty, které se vyskytnou a upozornit na ně v souladu s příslušnými zásadami a směrnicemi.

Tato politika je závazná pro všechny zaměstnance DPMB, a.s. a nabývá účinnost dnem vydání.

V Brně dne 27. listopadu 2024

Ing. Miloš Havránek
generální ředitel