# POLITIKA SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

| Verze: | Platnost od: | Počet stran: | Počet příloh: |
|---|---|---|---|
| **2.0** | **1.10.2026** | **1** | **0** |

Společnosti Brink‘s Cash Solutions (CZ), a.s. a Brink’s Cash Solutions Services(CZ) s.r.o. (obě dvě společnosti jsou dále v dokumentu uváděny jen jako „Brink‘s“), poskytují komplexní cash management služby zahrnující přepravu a zpracování hotovosti, obsluhu a servis bankomatů (ATM). Všechny činnosti jsou založeny na hodnotách, které jsou společné s mezinárodní skupinou Brink´s.

S ohledem na zpracování dat a informací musíme klást i důraz na bezpečnost a řízení přístupu k vnitřním informacím a k informacím zákazníků. Tím přispíváme nejen ke zvýšení úrovně zabezpečení dat, s nimiž společnost a její zaměstnanci pracují, ale k celkovému upevnění důvěryhodnosti společnosti.

V tomto směru vnímá důvěryhodnost vedení společnosti jako přidanou hodnotu pro zákazníka, který vnímá zázemí společnosti jako bezpečné a je spokojen s poskytnutou službou.

Sledujeme trvale nejnovější bezpečnostní hrozby i trendy v oblasti obrany proti nim a zajišťujeme tak prostředky pro plnění cílů v oblasti bezpečnosti informací a jejich pravidelným přezkoumáním směřujeme naše činnosti k trvalému zvyšování efektivity systému řízení bezpečnosti informací.

Systém řízení bezpečnosti informací je vystavěn na následujících zásadách:

- Ochrana dat smluvních partnerů.
- Zajištění ochrany osobních údajů v souladu s platnou legislativou.
- Vytváření a prosazování systému řízeného přístupu k informacím.
- Provádění stálé identifikace bezpečnostních rizik, incidentů a přijímání účinných opatření pro zlepšování bezpečnosti informací.
- Zajišťování systematického vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací.
- Zpracovávání opatření pro zachování kontinuity činnosti pro případy závažného výpadku v oblasti informací, pravidelné přezkušování a ověřování těchto opatření.
- Zabezpečování informačních systémů, internetu, elektronické pošty a dalších způsobů výměny informací přístupných veřejnosti.
- Zabezpečování systému fyzického přístupu do prostor společnosti.
- Nepřetržité zajišťování dostupnosti, spolehlivosti a integrity dat.
- Prosazování politiky bezpečného pracoviště, tzn. dodržování zásady čistého stolu, prázdné obrazovky a odpadkového koše bez zabezpečených informací.
- Dodržování bezpečnostních pravidel pro přenosná počítačová zařízení a jiné nosiče informací.
- Zajišťování spolehlivé kontroly celé interní sítě proti působení zlomyslného softwaru, spolehlivé chránění a zálohování informací.
- Sdělování a výměnu informací s třetí stranou provádět pouze na základě zákona, nebo na základě smlouvy uzavřené v písemné formě.

Tato politika je ve společnosti rozpracována do interních řídících dokumentů se stanovením odpovědností jednotlivých zaměstnanců.