Smernica o ochrane údajov a informačných technológií

Cieľ:
Vytvoriť jednotný rámec na ochranu IT zariadení, údajov a internej komunikácie organizácie SlavkaSk. Tým sa zabezpečí súlad s predpismi, minimalizujú sa bezpečnostné riziká a podporí sa bezpečné a nepretržité fungovanie organizácie.

1. Riadenie prístupových práv
• Každý zamestnanec má prístup k IT systémom len v rozsahu zodpovedajúcom jeho pracovnej pozícii.
• Prístupové práva sú zaznamenávané v centrálnom IT systéme a prehodnocujú sa štvrťročne.
• Prístup zamestnancov, ktorí boli prepustení alebo odišli, musí byť okamžite zrušený.

2. Používanie IT zariadení a internej siete
• Na pracovisku je povolené používať len zariadenia vo vlastníctve SlavkaSk (počítače, notebooky, telefóny a iné).
• Prístup k sieti je možný len cez heslom chránené a centrálne monitorované pripojenie.
• Je zakázané pripájať akékoľvek externé USB zariadenia, pamäťové kľúče alebo osobné úložiská bez písomného povolenia.

3. E-mail a interná komunikácia
• Oficiálne úradovanie môže prebiehať výlučne prostredníctvom e-mailových adries končiacich na **@slavkask.com**.
• Pri internej komunikácii sa zamestnanci musia vyhýbať neformálnym alebo dvojzmyselným výrazom.
• Všetky formy komunikácie (e-mail, chat, cloudové služby) sú chránené centrálnym systémom zálohovania a logovania.

4. Ochrana údajov a súlad s GDPR
• Každý zamestnanec je povinný dodržiavať nariadenia GDPR stanovené Európskou úniou.
• Osobné údaje sa smú spracovávať len na vopred určené účely a prístup k nim majú výlučne centrálne určení správcovia údajov.
• Pri prevádzke webstránok, kontakte so zákazníkmi a náborových procesoch sa používajú len schválené vyhlásenia o ochrane osobných údajov.

5. Dôvernosť a zaobchádzanie s citlivými informáciami
• Každý zamestnanec podpisuje pri nástupe do práce vyhlásenie o mlčanlivosti.
• Akékoľvek poskytovanie informácií tretím stranám, ich neoprávnené kopírovanie alebo odovzdávanie má za následok okamžité ukončenie pracovného pomeru.

• Aplikácie ako WhatsApp, Telegram, Signal a iné možno na pracovné účely používať len na základe internej dohody.

6. Správa kryptomien a blockchain technológie

• S kryptomenou **IGNA** môžu narábať výlučne určené osoby a len prostredníctvom **multisig** peňaženiek.

• Každá transakcia je zaznamenaná v samostatnom internom registri.

• Prístup k blockchain údajom **IGNA** podlieha samostatnému vyhláseniu o mlčanlivosti a riadi sa prísnym vnútorným schvaľovacím protokolom.

7. Pravidelné audity a kontroly

• Na každom pracovisku sa musí každého pol roka vykonať povinný audit IT bezpečnosti.

• Aktualizácie, údržbu a testovanie IT systémov vykonáva centrálny IT tím.

• Každé podozrivé správanie (krádež hesla, neoprávnený prístup) sa musí okamžite nahlásiť a prešetrí ho IT oddelenie.

8. Prevencia a obnova pri strate údajov

• Dokumenty sa automaticky zálohujú každý deň do zabezpečeného cloudového systému.

• V prípade straty údajov musia byť príslušné systémy obnovené do 24 hodín.

• Na zabezpečenie nepretržitej prevádzky funguje v každej krajine aspoň jeden bezpečnostný zrkadlový server.

Nariadenie vydal:
Ignác Czakó, predseda medzinárodnej neziskovej organizácie SlavkaSk