Adatbiztonsági és informatikai szabályzat

Cél:
Egységes keretrendszer létrehozása a SlavkaSk informatikai eszközeinek, adatainak és belső kommunikációjának védelmére. Ez biztosítja a szabályozási megfelelést, minimalizálja a biztonsági kockázatokat, és támogatja a szervezet biztonságos és folyamatos működését.

1. Hozzáférési jogosultságok szabályozása
• Minden dolgozó csak a munkakörének megfelelő mértékben férhet hozzá a számítástechnikai rendszerekhez.
• A hozzáférési jogosultságokat a központi IT-rendszer rögzíti, és negyedévente felülvizsgálja.
• Az elbocsátott vagy kilépő dolgozók hozzáférését azonnal meg kell szüntetni.

2. Informatikai eszközök és belső hálózat használata
• Minden munkahelyen kizárólag a SlavkaSk tulajdonában álló számítógépek, laptopok, telefonok és egyéb eszközök használhatók.
• A hálózatokhoz történő hozzáférés csak jelszóval védett, központilag monitorozott kapcsolaton keresztül történhet.
• Tilos bármilyen külső USB-eszköz, pendrive vagy személyes adattároló csatlakoztatása, kivéve **írásos engedéllyel**.

3. E-mail és belső kommunikáció
• A hivatalos ügyintézés kizárólag a @slavkask.com végződésű e-mail címekről történhet.
• Belső levelezésben a munkavállalóknak tartózkodniuk kell az informális vagy kétértelmű kifejezésektől.
• A kommunikáció minden formáját (e-mail, chat, felhőszolgáltatás) a központi rendszer biztonsági mentéssel és naplózással védi.

4. Adatvédelem és GDPR-megfelelés
• Minden munkavállaló köteles betartani az Európai Unió által meghatározott GDPR előírásokat.
• A személyes adatokat kizárólag célhoz kötötten lehet kezelni, és kizárólag a központilag kijelölt adatkezelők férhetnek hozzá.
• A weboldalakon, ügyfélkapcsolatokban és toborzásban is csak megfelelő adatvédelmi nyilatkozatokkal dolgozunk.

5. Titoktartás és bizalmas információk kezelése
• Minden dolgozó a munkába lépéskor titoktartási nyilatkozatot ír alá.
• Bármilyen információ harmadik félnek történő átadása, engedély nélküli másolása, továbbítása azonnali munkaviszony-megszüntetést von maga után.
• A WhatsApp, Telegram, Signal vagy más applikációk csak belső megegyezéssel használhatók munkacélra.

6. Kriptovaluta és blokklánc technológia kezelése

• Az IGNA kriptovaluta kezelése kizárólag a kijelölt személyek és multisig tárcákon keresztül történhet.

• Minden tranzakciót külön belső nyilvántartás kísér.

• Az IGNA blokklánc-adatokhoz való hozzáférés külön titoktartási nyilatkozat alá esik, és szigorú belső engedélyezési protokoll szerint történik.

7. Rendszeres audit és ellenőrzés

• Félévente kötelező IT-biztonsági auditot végezni minden telephelyen.

• Az informatikai rendszerek frissítését, karbantartását és tesztelését a központi IT-csapat végzi.

•Minden rendellenes viselkedést (jelszólopás, jogosulatlan belépés) azonnal jelenteni kell, és az IT részleg kivizsgálja.

8. Adatvesztés megelőzése és helyreállítás

• A dokumentumok naponta automatikusan mentésre kerülnek egy biztonságos felhőalapú rendszerben.

• Adatvesztés esetén 24 órán belül visszaállítható állapotba kell hozni az érintett rendszereket.

• A működésfolytonosság biztosítására minden országban legalább egy biztonsági tükörszerver működik.

A szabályozást elrendelte:
Czakó Ignác, **a SlavkaSk Nemzetközi Nonprofit Szervezet elnöke**