Internal Data Security & IT Policy

Purpose:
To establish a unified framework for protecting SlavkaSk's IT assets, data, and internal communications. It ensures regulatory compliance, minimizes security risks, and supports the organization's secure and continuous operation.

1. Access Rights Regulation
• All employees may access IT systems only to the extent necessary for their job duties.
• Access rights are recorded by the central IT system and reviewed quarterly.
• Access for terminated or resigning employees must be revoked immediately.

2. Use of IT Equipment and Internal Network
• Only SlavkaSk-owned computers, laptops, phones, and other devices may be used at the workplace.
• Network access is allowed only via password-protected, centrally monitored connections.
• Connecting any external USB devices, pendrives, or personal storage devices is prohibited **unless with written permission.**

3. Email and Internal Communication
• Official correspondence must use email addresses ending with @slavkask.com.
• Employees must avoid informal or ambiguous expressions in internal communications.
• All communication forms (email, chat, cloud services) are secured by centralized backup and logging.

4. Data Protection and GDPR Compliance
• All employees must comply with the GDPR regulations set by the European Union.
• Personal data may only be processed for specific purposes and accessed only by centrally designated data controllers.
• Websites, customer relations, and recruitment processes must use appropriate privacy statements.

5. Confidentiality and Handling of Sensitive Information
• All employees sign a confidentiality agreement upon starting employment.
• Unauthorized sharing, copying, or forwarding of information to third parties results in immediate termination.
• Use of WhatsApp, Telegram, Signal, or other apps for work purposes requires internal approval.

6. Cryptocurrency and Blockchain Technology Handling
• Management of IGNA cryptocurrency is restricted to designated personnel and multisig

wallets.
• All transactions are recorded in a separate internal ledger.
• Access to IGNA blockchain data is subject to a confidentiality agreement and strict internal authorization protocols.

7. Regular Audits and Inspections
• Mandatory IT security audits are conducted biannually at all sites.
• The central IT team manages system updates, maintenance, and testing.
• Any irregular behavior (password theft, unauthorized access) must be reported immediately and investigated by IT.

8. Data Loss Prevention and Recovery
• Documents are automatically backed up daily to a secure cloud-based system.
• In case of data loss, affected systems must be restored within 24 hours.
• To ensure business continuity, at least one backup mirror server operates in every country.

Regulation Issued By:
Ignác Czakó, President of the SlavkaSk International Nonprofit Organization