INFORMÁCIÓBIZTONSÁGI POLITIKA

— Neuron Software —

A NEURON Szoftver Korlátolt Felelősségű Társaság (továbbiakban: vállalat) menedzsmentje a működése és nyújtott szolgáltatásai területén az ügyfél és saját adatok védelmét, és az érdekelt felek információbiztonsági elvárásainak való folyamatos megfelelést meghatározó elemként kezeli. Mindezért a vállalati működése és bizalmi szolgáltatásaiban az MSZ ISO/IEC 27001:2023 szabvány követelményeit kielégítő információbiztonsági irányítási rendszert (továbbiakban: IBIR) épített ki, folyamatosan működteti és fejleszti.

POLITIKA CÉLJA ÉS HATÁLYA:

Az információbiztonság megvalósítása és hatékony működtetése a vállalati célok elérésének érdekében történik. Az információbiztonsági politikát a menedzsment elkötelezetten támogatja. Ez a politika biztosítja a biztonsági intézkedések hatékony működését beépülve a vállalat mindennapi folyamataiba, ezáltal része a szervezeti kultúrának.

FŐ CÉLKITŰZÉSEK:

1. **Adatok bizalmassága, sértetlensége és rendelkezésre állása:** A szervezet informatikai rendszereiben található adatok hitelességének és biztonságának megőrzése érdekében intézkedéseket vezetünk be.
2. **Ügyfelek adatainak biztonságos kezelése:** Az ügyfél, partneri, munkatársi és egyéb üzleti információk bizalmasságának biztosítása.
3. **Szolgáltatások információbiztonságának fenntartása:** Az ügyfeleknek nyújtott szolgáltatások magas minőségű és jól definiált információbiztonságának folyamatos biztosítása.
4. **Jogszabályi és szabályozási megfelelőség:** Az alkalmazott informatikai rendszerek és támogató folyamatok megfelelése a jogszabályi és egyéb szabályozási követelményeknek.
5. **Folyamatos fejlesztés:** Korszerű technológiák bevezetése, szervezeti folyamatok és szoftver fejlesztési, alkalmazás üzemeltetési és tanácsadói szolgáltatások folyamatos fejlesztése, a szabályozási követelmények, az ügyfelek és a piac igényei alapján.
6. **Szakmai kompetencia:** A legmagasabb szintű szakmai hozzáértés biztosítása folyamatos képzéssel.
7. **Megbízható alvállalkozók kiválasztása:** Megfelelő alvállalkozók alkalmazása, akik elfogadják és teljesítik az információbiztonsági követelményeket.
8. **Kockázatok minimalizálása:** A védendő információvagyon fenyegetettségének rendszeres felülvizsgálata és újraértékelése, az információbiztonsági előírások frissítése.
9. **Kiemelt incidensek elkerülése:** Elfogadhatatlannak tartjuk az ügyfelek adatainak nyilvánosságra kerülését, az adatvesztéseket, valamint a hálózati betöréseket.

CERTIFIED ISO 27001:2023 COMPANY