INFORMÁCIÓBIZTONSÁGI POLITIKA

A **RISE Business Solutions Kft.** (továbbiakban: Társaság) vezetősége elkötelezett az információk, informatikai rendszerek és a kapcsolódó szolgáltatások biztonságának fenntartása és folyamatos fejlesztése mellett. A Társaság célja, hogy az általa kezelt információk és információfeldolgozó rendszerek – beleértve a felhőalapú szolgáltatásokat és környezeteket is – bizalmasságának, sértetlenségének és rendelkezésre állásának minden körülmények között biztosított legyen, összhangban az üzleti, jogszabályi, szerződéses és szabványi követelményekkel.

Jelen Politika hatálya kiterjed a Társaság teljes információs és informatikai környezetére, a felhőalapú szolgáltatások igénybevételére és nyújtására, továbbá minden munkavállalóra, szerződött partnerre, beszállítóra és egyéb érintettre.

A Társaság az információbiztonságot kockázatalapú megközelítéssel kezeli, amelynek során az alkalmazott védelmi intézkedések az információk érzékenységével, az üzleti kockázatokkal, valamint a fenyegetettségek és sérülékenységek mértékével arányosan kerülnek meghatározásra. A kockázatkezelési folyamat eredményeit a vezetőség rendszeresen felülvizsgálja.

A Társaság a felhőszolgáltatások esetében alkalmazza a megosztott felelősségi modellt, amelyben a felelősségi határok a felhőszolgáltató és a Társaság között egyértelműen meghatározásra és dokumentálásra kerülnek. Ennek keretében a Társaság felelős az általa kezelt adatok, hozzáférések, konfigurációk és alkalmazások biztonságáért.

A Társaság biztosítja, hogy a biztonsági követelmények már a rendszerek tervezési és bevezetési szakaszában érvényesüljenek és a működés során folyamatos felülvizsgálat mellett megfeleljenek a jogszabályi, szabványi és szerződéses elvárásoknak.

A Társaság kezelésében működő infokommunikációs-, informatikai- és információs rendszerek tervezésére, bevezetésére, üzemeltetésére és ellenőrzésére vonatkozó feladatokat úgy kell elvégezni, hogy a rendszerek védelme a jogszabályi előírásoknak megfeleljen, valamint a védelem költsége a potenciális kárértékkel arányos legyen.
Ennek érdekében:

- Megterveztük, kiépítettük és folyamatosan fejlesztjük az MSZ ISO/IEC 27001:2023 szabvány szerinti Információbiztonsági Irányítási Rendszerünket (IBIR), figyelembe véve a felhőalapú szolgáltatásokra vonatkozó ISO/IEC 27017 és 27018 ajánlásokat.
- Gondoskodunk az információbiztonsági események előfordulásának csökkentéséről, az incidensek dokumentált kivizsgálásáról, valamint a jogszabályok szerinti jelentési kötelezettségek teljesítéséről.
- Biztosítjuk, hogy a felhasználók tisztában legyenek az információbiztonsági fenyegetésekkel és a rájuk vonatkozó szabályokkal.
- Megvédjük az információkat és az információfeldolgozó eszközöket a jogosulatlan hozzáféréstől, módosítástól, elvesztéstől és megsemmisüléstől, beleértve a felhőalapú környezeteket is.
- A rendszerek üzemeltetését és változáskezelését dokumentált eljárások alapján végezzük, biztosítva a változások nyomon követhetőségét és ellenőrizhetőségét.
- Az új információs rendszerek beszerzését és a meglévő rendszerek fejlesztését az információbiztonsági szempontok maradéktalan figyelembevételével végezzük.
- Rendszeresen meghatározunk és felülvizsgálunk mérhető információbiztonsági célokat, amelyek támogatják az IBIR folyamatos fejlesztését.
- Elkötelezettek vagyunk a személyes adatok kezeléséről és védelméről szóló EU-s és tagállami jogszabályok, valamint a Társaság szolgáltatásait igénybe vevő ügyfelek szerződéseiben rögzített személyes adatkezelésre vonatkozó egyedi elvárások betartása mellett.

- Felhőszolgáltatás nyújtása esetén biztosítjuk, hogy az ügyféladatok bizalmassága, sértetlensége és rendelkezésre állása megfeleljen az iparági sztenderdeknek és az ISO/IEC 27017, 27018 elvárásainak.
- Gondoskodunk arról, hogy a felhőszolgáltatások esetében a megosztott felelősségi modell egyértelműen meghatározásra és dokumentálásra kerüljön.
- Gondoskodunk arról, hogy az engedélyezett bennfentesekből (ideértve az adatokhoz hozzáférő belső és külső munkatársakat, valamint beszállítókat) eredő kockázatokat azonosítsuk, értékeljük és kezeljük. A hozzáférések a szükséges minimumra korlátozódnak, rendszeresen felülvizsgálatra kerülnek és minden privilegizált követelmény naplózásra kerül.
- Gondoskodunk arról, hogy a felhasználók adatainak tárolása logikailag elkülönítetten, több-bérlős környezetben is megfelelő védelmi intézkedésekkel történjen.
- Biztosítjuk, hogy a felhőszolgáltatás ügyféladataihoz kizárólag az arra felhatalmazott személyek férjenek hozzá és minden hozzáférés naplózásra kerüljön. A hozzáférési jogosultságokat rendszeresen felülvizsgáljuk, hogy csak a szükséges mértékű hozzáférés maradjon érvényben. Az ügyféladatok védelmét kockázatarányos technikai és szervezési intézkedésekkel biztosítjuk, összhangban a hozzáférés-kezelési elvekkel és az adatvédelem követelményeivel.
- A privilegizált és adminisztratív hozzáférések esetében kockázatarányos kontrollokat alkalmazunk (pl. erős hitelesítés, naplózás, rendszeres felülvizsgálat).
- Gondoskodunk arról, hogy a felhőszolgáltatást igénybe vevő ügyfelek fiókjainak teljes életciklusa – létrehozás, módosítás, felfüggesztés, megszüntetés – szabályozott és dokumentált folyamatok alapján történjen. A jogosultságok kiosztása és visszavonása ellenőrzött módon zajlik, biztosítva a minimálisan szükséges hozzáférést.
- A felhőszolgáltatásokat érintő változások – különösen a biztonsági, konfigurációs vagy működési módosítások – esetén biztosítjuk, hogy az ügyfelek időben, átlátható módon tájékoztatást kapjanak. A kommunikáció tartalmazza a változás jellegét, hatását és az esetleges ügyféloldali teendőket.
- A virtualizációs környezetekben biztosítjuk a logikai elkülönítést, a kockázatok kezelését, valamint a virtuális gépek és konténerek biztonságos konfigurációját. A virtualizációs réteghez való hozzáférés szigorúan kontrollált és naplózott, a konfigurációk változásai pedig dokumentált módon követhetők.
- A felhasználói fiókok teljes életciklusát kontrollált módon kezeljük.
- Gondoskodunk a felhőszolgáltatások naplózásáról, monitorozásáról és az események rendszeres elemzéséről.
- Információbiztonsági incidens esetén haladéktalanul tájékoztatjuk az érintett ügyfeleket és a vizsgálatok támogatása érdekében – a jogszabályi és szerződéses keretek között – együttműködünk a hatóságokkal és az ügyfelekkel. A törvényszéki vizsgálatokhoz szükséges naplóadatok és releváns információk megőrzése és átadása szabályozott módon történik.
- A felhasználókat tájékoztatjuk a felhőszolgáltatások használatának sajátosságairól, különös tekintettel a szolgáltatói hozzáférésekre, a több-bérlős működésre és a privilegizált hozzáférésekre.
- Felhőszolgáltatás igénybevétele során biztosítjuk, hogy a hozzáférések korlátozottak legyenek, a konfigurációk biztonságosak maradjanak, a kockázatkezelés folyamatos legyen és a felhőszolgáltató csak megfelelő biztonsági és jogi környezetben működjön.
- Az adatok tárolása és feldolgozása kizárólag olyan földrajzi helyeken történik, amelyek megfelelnek az EU és a vonatkozó jogszabályi követelményeknek.

Kelt: Budapest, 2026.08.31.

Fónai Tamás Zsolt ügyvezető és
Győri Márta műszaki igazgató
RISE Business Solutions Kft.