KELER Központi Értéktár Zrt.

KELER Zrt. 9-10 számú értéktári leirat

A KELER Zrt. által vélt vagy észlelt csalás vagy biztonsági fenyegetések esetén az ügyfelek értesítésére szolgáló biztonságos eljárásokról

Hatályba lépés dátuma: 2023. május 10.

Tisztelt Ügyfeleink!

Jelen értéktári leirat tartalmazza a KELER Zrt. által vélt vagy észlelt csalás vagy biztonsági fenyegetések esetén az Ügyfelek értesítésére szolgáló biztonságos eljárásra vonatkozó információkat.

A KELER Csoport meglévő eszköztárából különböző, a belső kontrollok és az (információ)biztonság körébe tartozó eszközöket, módszereket alkalmaz a visszaélések, illetve különböző biztonsági fenyegetések megelőzése érdekében. A bevezetett eljárások és biztonsági környezet MSZ ISO/IEC 27001:2014 minősítése is tanúsítja a KELER Zrt. elkötelezetségét az információbiztonság területén.

a) Információbiztonsági eszközök, módszerek

- Fizikai biztonság
- Hálózatbiztonság
- Végpontvédelem
- Adatbiztonság
- Felhasználói és hozzáférés kezelés
- Adatcenter és szerver biztonság
- Biztonsági monitoring és választerület
- Biztonsági oktatás és tudatosság
- Szabályozás /megfelelés (auditok, penetrációs testek)ű
- Üzletmenet-folytonosság

b) Belső kontroll eszközök, módszerek

- belső kontrollrendszer (például „négy szem" elv) működtetése,
- a folyamatba épített, valamint az előzetes és az utólagos vezetői ellenőrzések,
- a független belső ellenőrzési tevékenység,
- a megfelelés ellenőrzési (compliance) tevékenység,
- megfelelő helyettesítési rendszer,
- visszaélés bejelentő rendszer (whistleblowing)
- személyes ügyletek szigorú szabályozása (Összeférhetetlenségi szabályzat, belső információval kapcsolatos ügylet tilalma).

A KELER Zrt. az általa esetlegesen vélt vagy észlelt csalás vagy biztonsági fenyegetések esetén kellő időben, az alábbiak szerint értesíti Ügyfeleit arról, hogy milyen biztonsági eljárást vezet be és/vagy milyen biztonsági eljárást vár el az Ügyfelektől (felhasználóktól) a biztonságos használat érdekében.

1. Abban az esetben, ha az érintett Ügyfelek köre jól behatárolható, a szerződéskötéskor megadott felhasználói elektronikus levélcímre küldött elektronikus értesítéssel, továbbá az eset súlyosságának függvényében a szerződéskötéskor megadott felhasználói telefonszámon is megkísérli az értesítést.

2. Abban az esetben, ha az Ügyfelek tömeges érintettsége áll fent, a KELER Zrt. a honlapján és a KID (KELER Interface Device) rendszerben megjelenő hirdetményben teszi közzé a vonatkozó információkat. Ezen felül, indokolt esetben a KELER kapcsolattartói listáján szereplő elektronikus levélcímekre küldött elektronikus levél útján is értesíti Ügyfeleit, valamint krízis esetén az Ügyfelek gyors tájékoztatása érdekében Teams csatornát nyit a KELER és annak elérhetőségét elektronikus levél útján küldi el Ügyfeleinek.

Az Ügyfelek kötelesek rendszeresen nyomon követni a KELER Zrt. honlapján (https://www.keler.hu) és a KID rendszerben a fentiek szerint nyújtott értesítéseket és az értesítésnek megfelelően eljárni.

A KELER Zrt. semmilyen célból nem kér az Ügyfeleitől elektronikus levélben, vagy telefonon, vagy SMS-ben jelszavakat, vagy belépési kódokat, sem más bizalmas adatokat.

Fontos, hogy semmilyen körülmények között ne adják ki személyes adataikat, azonosítóikat, jelszavaikat, belépési kódjaikat!

A nem megfelelő felhasználásból – pl. felhasználónév és jelszó/belépési kód titokban tartásának hiánya – eredő esetleges károkért a KELER Zrt. nem vállal felelősséget.

KELER Zrt.