A TRIGO tisztában van azzal, hogy az információfeldolgozás kulcsfontosságú a szolgáltatásai nyújtásához, és hogy gondoskodni kell az összegyűjtött, feldolgozott és megosztott információk biztonságáról és védelméről. Vezetőségünk elkötelezett amellett, hogy nemcsak biztosítsa az alkalmazandó követelmények (jogi, szabályozási, valamint az ügyfelek, beszállítók, munkavállalók és egyéb érdekelt felek által támasztott követelmények) betartását, hanem folyamatosan fejlessze az irányítási rendszert is az érzékeny információk rendelkezésre állásának, integritásának és titkosságának biztosítása érdekében.

Ennek érdekében törekszünk a következőkre:

- Az információbiztonsági kockázatok és lehetőségek azonosítására és kezelésére.
- A munkatársak figyelmét felhívjuk a kockázatokra, és képzések, kommunikáció és a tanulságok megosztása révén kialakítjuk az információbiztonsági kultúrát, hogy szervezetünk minden munkatársa naprakész legyen a legjobb biztonsági gyakorlatok terén.
  → A TRIGO célja, hogy 2027 végéig munkatársainak legalább 90%-a részt vegyen kiberbiztonsági képzésen.
- A személyes adatok védelme a jogi kötelezettségeinknek megfelelően.
- Stabil, biztonságos és magas rendelkezésre állású informatikai infrastruktúrák és digitális rendszerek bevezetése és karbantartása, átfogó kiberbiztonsági stratégia támogatásával, beleértve a kiszervezett folyamatok ellenőrzését is.
- Az információbiztonsági incidensek hatékony felismerése, jelentése és kezelése.
- Stabil, biztonságos és magas rendelkezésre állású IT-infrastruktúrák és digitális rendszerek üzembe helyezése és karbantartása, átfogó kiberbiztonsági stratégia támogatásával, beleértve a kiszervezett folyamatok ellenőrzését is.
- Folyamatosan figyelemmel kísérjük informatikai környezetünket belső felügyeleti eszközök és külső kiberbiztonsági értékelő platformok kombinációjával, amelyek folyamatos áttekintést nyújtanak a sebezhetőségeknek és fenyegetéseknek való kitettségünkről.
  → A TRIGO célja, hogy független kiberbiztonsági értékelő platformok mérései alapján legalább 750-es értékelést érjen el az 1000-ből, ami tükrözi a külső támadási felület szilárd ellenőrzését, valamint a sebezhetőségek azonosítására és kijavítására irányuló folyamatos erőfeszítéseket.
- Rendszeres biztonsági auditokat végzünk a bevezetett ellenőrzések hatékonyságának biztosítása és a folyamatos fejlesztés ösztönzése érdekében.
- Kipróbáljuk és karbantartjuk az operatív IT-rendszereinkre vonatkozó katasztrófa-helyreállítási terveket.

Ezt az irányelvet az információbiztonsági vezető dolgozza ki a csoport adatvédelmi tisztviselőjével együttműködve, és a vezérigazgató, valamint a vezérigazgató-helyettes hagyja jóvá. Az irányelv végrehajtását számos irányelv, folyamat és erőforrás támogatja.

A szabályzat a TRIGO világszerte működő valamennyi szervezetére vonatkozik, beleértve az összes alkalmazottat, alvállalkozót és harmadik felet, akik hozzáférnek a TRIGO információs rendszereihez.

Végrehajtása egy megosztott felelősségi modellen alapul:

- A csoport informatikai részlege felelős a globális informatikai infrastruktúrák, a kiberbiztonsági intézkedések, a felügyeleti tevékenységek és a katasztrófa-helyreállítási képességek meghatározásáért, bevezetéséért és karbantartásáért.
- A helyi szervezetek és a felhasználók felelősek a meghatározott szabályok betartásáért, az információs eszközök védelméért, valamint az információbiztonsági kockázatok és incidensek kezeléséhez való hozzájárulásért.

Ezért, bár egyes ellenőrzési intézkedéseket központilag, csoportszinten kezelnek, az egyes szervezetek ügyvezető igazgatója felelős a jelen irányelvnek a saját hatáskörén belüli megfelelő alkalmazásáért.

A Csoport emellett elősegíti a folyamatos fejlesztést a releváns mutatók nyomon követésével és szükség esetén korrekciós intézkedések végrehajtásával.

Ezt a szabályzatot a vezetői felülvizsgálati folyamat részeként évente felülvizsgálják. A felülvizsgálat során figyelembe veszik a belső és külső kérdéseket, a jelentős biztonsági eseményeket és azok hatásait, valamint a Csoport stratégiai irányvonalát, annak érdekében, hogy biztosítsák a szabályzat folyamatos relevanciáját, hatékonyságát és folyamatos fejlesztését.

Számítunk arra, hogy minden munkatársunk helyes magatartást tanúsít, és javítási javaslatok benyújtásával hozzájárul biztonsági gyakorlataink fejlesztéséhez.

Matthieu RAMBAUD
Vezérigazgató

Benoît LEBLANC
Vezérigazgató helyettes

Verzió	Hatálybalépés dátuma	Oldal	A változások leírása
A	2026.07.15	Mind	A tartalom eredetileg a PR.MAN.WW.09.EN-A „Információbiztonság” című dokumentumban szerepelt (2023. április 3-i változat). Ez az új dokumentum mennyiségi célokat is meghatároz.