

Információbiztonsági irányelvek

Az információkezelés szabványosítása, az információbiztonság biztosítása.

Az információtechnológia fejlesztése, a vállalati működés támogatása.

1. Szervezeti szintű tudatosság

Az információbiztonsági irányítás kulcseleme az ember. A vállalat információbiztonságának elsődleges feladata az összes munkavállaló információbiztonsági tudatosságának növelése. Képzések, oktatás és a felelősségek egyértelmű meghatározása révén az információbiztonsági tevékenység az egyének szintjén valósul meg.

2. Biztonsági kontroll

Az információbiztonsági irányítás az információbiztonsági kontrollok alkalmazásán alapul. A vállalat K+F eredményeinek, ügyféladatainak, működési adatainak és egyéb érzékeny információinak védelme a megbízható információbiztonsági gyakorlatoktól függ. A felelősségi körök egyértelmű meghatározásával és a technológiai intézkedések (kontrollok) bevezetésével biztosítjuk a strukturált folyamatokat, a szabványosított eljárásokat, a megfelelő eszközhasználatot, az ellenőrzéseket és a folyamatos fejlesztést.

3. Kockázatkezelés

Az információbiztonság célja a kockázatok csökkentése. Irányadó elvünk, hogy az információbiztonsági incidensekből eredő veszteségeket elfogadható szinten tartjuk, illetve olyan információbiztonsági védelmi képességeket alakítsunk ki, amelyek összhangban állnak az üzleti digitalizáció fejlődésével.

4. Az üzlet védelme

Az információbiztonság középpontjában a termelés működésének támogatása áll. Minden információbiztonsági tevékenységnek a termelési és üzleti folyamatok köré kell szerveződnie. Technológiai védelmi intézkedéseket alkalmazunk a termékek folyamatos és stabil gyártásának és szállításának biztosítása érdekében.

Információbiztonsági célok

Az európai és magyarországi kiberbiztonsági és adatvédelmi megfelelési követelmények teljesítése, továbbá az egyre kifinomultabb és összetettebb kiberfenyegetések kezelése érdekében az információbiztonság megerősítése a vállalat kiemelt feladatává vált. Ennek megfelelően az alábbi információbiztonsági célokat határoztuk meg.

Titoktartási cél

A vállalat szigorúan titkos és bizalmas információinak, dokumentumainak és anyagainak védelme az illetéktelen hozzáféréssel szemben.
Éves információszivárgási incidensek száma: ≤ 4 alkalom/év.

Integritási cél

A vállalati termelési adatok adatvesztése bármely okból: ≤ 1 alkalom/év.
A maximális adatvesztés nem haladhatja meg a 24 órát, azaz RPO ≤ 24 óra.

Rendelkezésre állási cél

Az alapvető üzleti rendszerek 7×24×365 üzemmódban működjenek.
Az éves összes megengedett leállási idő nem haladhatja meg az 526 percet.

Megfelelőség

Megfelelés a globális információbiztonsági jogszabályoknak és előírásoknak, és a jogsértésekből eredő hatósági bírságok elkerülése.

Képzés

Az információbiztonsági tudatossági képzés terjedjen ki az összes munkavállalóra, 100%-os lefedettséggel.

E célok elérése érdekében folyamatosan fejlesztjük információbiztonsági ellenállóképességünket a kiberfenyegetések hatékony kezelése érdekében. A munkavállalói tudatosság növelése érdekében rendszeres információbiztonsági képzéseket és tudatosságnövelő kampányokat szervezünk. Információbiztonsági irányelveket, eljárásokat és rendszereket vezettünk be a vállalati információbiztonság megerősítése, valamint az ügyfelek és partnerek számára biztonságosabb üzleti környezet megteremtése céljából.

Irányítási intézkedések

A vállalat információbiztonsági irányításának folyamatos fejlesztése és a hosszú távú versenyelőnyök megalapozása érdekében, az alábbi szabványokkal összhangban:

- Nemzetközi Szabványügyi Szervezet / Nemzetközi Elektrotechnikai Bizottság ISO/IEC 27001:2022 Információbiztonság, kiberbiztonság és adatvédelem — Információbiztonsági irányítási rendszerek — Követelmények
- ISO/IEC 27002:2022 Információbiztonság, kiberbiztonság és adatvédelem — Információbiztonsági kontrollok

- VDA ISA (TISAX® követelmények)

információbiztonsági irányítási szabályzatok sorozatát adtuk ki és vezettük be. A vállalat megszerezte a TISAX® információbiztonsági tanúsítást (Trusted Information Security Assessment Exchange), létrehozta az Információbiztonsági Irányítási Rendszert (ISMS), és megfelel a VDA ISA követelményeinek.

Az információbiztonsági irányítóbizottság és az információbiztonsági vezető (CISO) irányításával évente belső információbiztonsági auditokat végzünk. Teljes körűen feltérképezzük a vállalat információs eszközeit, és kockázatértékelést végzünk, amelyek eredményeként információs eszköz kockázatértékelési nyilvántartások, kockázatértékelési jelentések és maradványkockázat-jóváhagyási jelentések készülnek. Az érintett belső szervezeti egységek objektív és dokumentált auditokat végeznek az információkezelés és az információs rendszerek biztonsági kockázatainak értékelésére, és a feltárt hiányosságok alapján haladéktalanul korrekációs intézkedéseket hoznak a szervezeti információbiztonsági követelmények teljesítése érdekében. Kritikus rendszerek vagy információk esetén az ellenőrzések közvetlenül a CISO felügyelete mellett történnek a megbízható és objektív kockázatellenőrzés biztosítása érdekében.

Elkészítettük a csoportszintű üzleti hatáselemzési (BIA) jelentést, és hároméves üzletmenet-folytonossági tervet hoztunk létre. Vészhelyzeti reagálási terveket készítünk, vészhelyzeti gyakorlatokat tartunk, és ezekről jegyzőkönyvet vezetünk az üzletileg kritikus rendszerek biztonságos és stabil működése, valamint az üzletmenet folytonosságának biztosítása érdekében.

Minden munkavállaló számára információbiztonsági képzéseket biztosítunk a biztonságtudatosság erősítése, a proaktív biztonsági kultúra kialakítása, valamint az információbiztonsági incidensek szabályszerű rögzítésének és jelentésének elősegítése érdekében.

Többszintű biztonsági mentési stratégiát dolgoztunk ki, és professzionális biztonsági mentési eszközöket szereztünk be a helyi és telephelyen kívüli biztonsági mentések elvégzéséhez. Rendszeresen végzünk biztonsági mentés-visszaállítási gyakorlatokat, hogy az adatvesztés és az RPO ne haladja meg a 24 órát. A hálózatbiztonság további fejlesztése érdekében átfogó biztonsági keretrendszert alakítottunk ki.

Az EU-s és magyar előírásokkal összhangban információbiztonsági

incidensmenedzsment rendszereket és folyamatokat vezettünk be, többek között:

- Irányelv az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2 irányelv)
- A kritikus szervezetek rezilienciájáról szóló irányelv (CER-irányelv)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

Ezek a keretrendszerek biztosítják, hogy információbiztonsági incidens esetén szervezetünk időben reagáljon, helyreállítsa a rendszert, és megfelelő időben értesítse az érintett belső és külső stakeholdereket.

Információbiztonsági kapcsolattartó e-mail-címe: tisax@hybernenergy.hu