

---

## INFORMÁCIÓBIZTONSÁGI POLITIKA

---

A ZÖLD HÍD B.I.G.G. NONPROFIT KFT-nél elköteleztük magunkat, hogy a hulladékgyűjtési és hulladékkezelési tevékenységeinket a legjobb minőségben nyújtjuk, a meghatározott információbiztonsági intézkedéseink betartásával, ezért megismertük és cégünk minden munkatársában tudatosítottuk a partnereink információbiztonságra vonatkozó legfontosabb követelményeit, melyek:

- a kezelt adatok és információk bizalmassága,
- külső hozzáférések megfelelő korlátozása,
- megbízható munkatársak alkalmazása, valamint
- a szolgáltatás folyamatos rendelkezésre állásának biztosítása.

Ennek megfelelően tevékenységünk biztonsága igen erős vevői elvárás, így ez az alapvető és elemi érdekünk, ezért az információbiztonsági stratégiánkban elsődleges szempont a cégünk informatikai és egyéb információs erőforrásainak, valamint a társaság működése szempontjából rendkívüli fontosságú adatainak, információinak védelme a **bizalmasság**, a **sértetlenség** szempontjából.

Cégünk működésével kapcsolatos szakmai elvárások nagyfokú rugalmasságot követelnek a saját belső működésünket illetően, így ezen a területen az információk **rendelkezésre állását** tekintjük alapvető szempontnak. Ennek érdekében szervezetünkön belül nyitottságot biztosítunk, munkatársaink részére elérhetővé tesszük a munkájukhoz szükséges információkat. Ez a bizalmi alapon való működési mód azt igényli, hogy az információbiztonsági elveket tudatosítsuk és azokat minden munkatársunk kötelező érvénnyel betartsa.

A Zöld Híd B.I.G.G. NONPROFIT KFT. alkalmazási területén és kezelésében működő informatikai és információs rendszerek tervezésére, bevezetésére, üzemeltetésére és ellenőrzésére vonatkozó feladatokat úgy végezzük el, hogy a rendszereink védelme a jogszabályi előírásoknak eleget tegyen, valamint a védelem hiányából eredő kockázatokkal legyen arányos.

Biztosítjuk az információk és az információ feldolgozási folyamatok bizalmasságát, sértetlenségét, rendelkezésre állását, azonosító és ellenőrző folyamatok kialakításával, folyamatba építésével és azok rendszeres felülvizsgálatával.

### **Szervezetbiztonságunk**

Az információbiztonságot úgy irányítjuk a szervezeten belül, hogy ezzel kezdeményezzük, fenntartsuk és ellenőrizzük az információbiztonság megvalósítását.

Fenntartjuk a biztonságát a szervezet azon információ-feldolgozó eszközeinek és információs vagyonának, amelyek a harmadik fél számára hozzáférhetőek úgy, hogy a szervezet információ-feldolgozó eszközeit korlátozott és ellenőrizhető módon tesszük hozzáférhetővé harmadik fél számára.

Fenntartjuk az információ biztonságát akkor is, ha az információfeldolgozási felelősséget más szervezetnek alvállalkozásba adjuk át.

---

**INFORMÁCIÓBIZTONSÁGI POLITIKA**

---

**Kockázatkezelésünk**

A kockázatkezelésünk során a meglévő vagyontárgyak meghatározását követően megállapítjuk a valós sérülékeny pontokat. A fenyegetés bekövetkezési gyakoriságának és a sérülékeny ponttal történő találkozás valószínűségének értékeivel együtt határozzuk meg a kockázat mértékét, a valószínűsített esemény hatásának figyelembevételével. Az intézkedéseket ennek megfelelően úgy hozzuk meg, hogy annak költségei egyensúlyban legyenek a becsült üzleti veszteségekkel.

**Munkatársaink információbiztonsági szerepe**

Gondoskodunk arról, hogy a munkatársaink felkészültek legyenek egy esetleges információbiztonságot érintő esemény bekövetkezésekor, valamint tudatosítjuk bennük az információbiztonsági szerepük fontosságát.

Oktatásokkal és folyamatos ellenőrzésekkel biztosítjuk, hogy a munkatársaink a szervezet információbiztonsági előírásait a szokásos napi munkájuk során betartsák.

**Fizikai és környezeti biztonságunk**

Megelőzzük az információs vagyon elvesztését, sérülését vagy veszélyeztetését, valamint az üzleti tevékenységek megszakadását úgy, hogy az információs vagyont fizikailag védjük a biztonsági fenyegetésektől és a környezeti veszélyektől. Fenntartjuk a szervezet vagyonának megfelelő védelmét és a veszteségeket minimalizáló óvintézkedéseket hozunk.

**Kommunikációnk és az üzemeltetés irányítása**

Gondoskodunk az információ-feldolgozó eszközök pontos és biztonságos működéséről dokumentált üzemeltetési eljárások betartásával és betartatásával, a változások ellenőrzésével, a rendszer-meghibásodások kockázatának minimalizálásával, rosszindulatú szoftverek elleni védekezéssel, az információfeldolgozás rendszergazda által történő állandó felügyeletével, valamint olyan hálózatok biztonsági menedzselésével, amelyek túlnyúlnak a szervezeti határokon.

**Hozzáférési politikánk**

Az információhoz és az üzleti folyamatokhoz való hozzáférést az üzleti és biztonsági követelmények alapján határozzuk meg és az alkalmazás során folyamatosan ellenőrizzük és naplózuk a bejelentkezést, illetve a hozzáférést.

**Az információs rendszereink beszerzése, fejlesztése, és fenntartása**

Az új információs rendszerek beszerzését, vagy a meglévő információs rendszerek fejlesztését, fenntartását úgy végezzük, hogy az információbiztonság valamennyi alapelve az információs rendszerekben megvalósuljon.

**Információbiztonsági incidenseink kezelése**

Az információbiztonsággal összefüggő incidenseket következetes és hatékony folyamat keretében kezeljük, az egyértelmű felelősségi viszonyok megjelölésével.

**Az üzletmenet-folytonosság biztosítása**

Célunk leküzdeni az üzleti tevékenységek megszakadásait és megvédeni a kritikus üzleti folyamatokat a nagyobb meghibásodások és katasztrófák hatásaitól.

---

**INFORMÁCIÓBIZTONSÁGI POLITIKA**

---

Konkrét tervek kidolgozásával gondoskodunk arról, hogy a biztonsági események bekövetkezése után a visszaállítási- és helyreállítási folyamatok zökkenőmentesek legyenek, valamint a zavarok okozta anyagi kár és időkiesés minimális legyen.

**Követelményeknek való megfelelés**

Célunk elkerülni bármely büntetőjogi, a törvényes, illetve szabályozói vagy szerződéses kötelezettségnek, valamint bármely biztonsági követelménynek a megszegését. Éppen ezért az információs rendszer biztonságát időről időre felülvizsgáljuk.

**Alkalmazási terület**

Tárgyi hatálya:

- A szervezeténél lévő adatok teljes körére, keletkezésük, felhasználásuk, feldolgozási helyük és megjelenési formájuktól függetlenül, továbbá bármely szervezeti egység birtokában szereplő hardver- és szoftver eszközre, beleértve az eszközök műszaki dokumentációját is.
- A szervezet tulajdonában lévő, vagy általuk tárolt valamennyi informatikai berendezésre, beleértve a berendezések műszaki dokumentációját is;
- A rendszerprogramokra és a felhasználói programokra;
- Az adathordozókra, azok tárolására és felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhöz történő eljuttatás folyamatait is;
- Az informatikai folyamatban szereplő valamennyi dokumentációra;
- Az adatok felhasználására vonatkozó utasításokra.

Területi, működési és személyi hatálya a Vezetői nyilatkozatunkban.

**Elkötelezettség**

Az **Információbiztonsági Politikánk** elveinek érvényesítését egyéb részletes szabályzatok, intézkedési eljárások, végrehajtási utasítások, irányelvek, kiadásával valósítottuk meg.

Minden eszközünkkel és tudásunkkal azt a célt szolgáljuk, hogy az ügyfeleink által ránk bízott vagy tudomásunkra jutott információk esetén megőrizzük azok bizalmasságát, sértetlenségét és rendelkezésre állását.

Vezetésünk elkötelezett a hatályos nemzeti és nemzetközi jogszabályoknak való megfelelésért, továbbá a nemzetközi normákhoz igazodó ISO 27001:2014 információbiztonsági irányítási rendszer folyamatos üzemeltetéséért és folyamatos továbbfejlesztéséért.

---

## **INFORMÁCIÓBIZTONSÁGI POLITIKA**

---

A ZÖLD HÍD B.I.G.G. NONPROFIT KFT. valamennyi alkalmazottjának ragaszkodnia kell a cég **Információbiztonsági Politikájához**, valamint szabályozó dokumentumok előírásaihoz és a megfogalmazott információbiztonsági intézkedésekhez.

Ezen dokumentum aláírásával személyesen is megerősítem az **Információbiztonsági Politikánk** melletti elkötelezettségünket.

Gödöllő, 2021.06.01.

Agatics Roland  
ügyvezető