Információbiztonsági Politika

Verzió	1.0
Dokumentum felelős	
Utoljára módosítva	2022. december 09.

Jóváhagyom:

2022. december 09.

Polgári István
Ügyvezető

V-Busz Veszprémi Közlekedési Kft.
8200 Veszprém, Házgyári út 1.
Cégjegyzékszám: 19 09 519972
Adószám: 26391546-2-19
www.vbusz.hu

Ezen szabályozás mindenkor érvényes, ellenőrzött példánya a V-Busz Veszprémi Közlekedési Korlátolt Felelősségű Társaság számítógépes hálózatán található.

A korábban kinyomtatott példányok érvényességét használat előtt összehasonlítással ellenőrizze!

TARTALOM

1 VEZETŐI ELKÖTELEZETTSÉG

A V-Busz Veszprémi Közlekedési Korlátolt Felelősségű Társaság (a továbbiakban Társaság) vezetésének szilárd meggyőződése, hogy az információ az ügyfelek és a Társaság olyan vagyona, amelyet védeni kell a különböző fenyegetések ellen, a bizalmasság, a sértetlenség és a rendelkezésre állás, illetve az üzletmenet folytonosságának biztosítása érdekében.

Ennek érdekében a Társaság legfelső vezetése a mindenkori üzleti és informatikai stratégiáját szem előtt tartva a jelen Informatikai Biztonsági Politikában (a továbbiakban IBP) meghatározott egyetemleges alapelvek és belső biztonsági alapkövetelmények maradéktalan teljesítését várja el a vezetőségtől, valamennyi munkatársától, beszállítóitól és minden egyéb érdekelt féltől. A jelen informatikai biztonságpolitika kivétel nélkül kiterjed a Társaság által végzett valamennyi folyamatra, valamennyi szervezeti egységre és telephelyre. A legfelső vezetés biztosítja a teljesítéshez alapvetően szükséges erőforrásokat.

2 CÉL

A Társaság a belső szabályozások magas szintű kezelése és menedzselése, a hazai és nemzetközi minőségirányítási sztenderdeknek és jogszabályoknak, valamint az ügyfeleknek nyújtott szolgáltatások átlátható kezelése érdekében elkészítette a jelen IBP-t.

Az IBP a Társaság vezetésének dokumentált akaratnyilvánítása a szervezet informatikai rendszerei által kezelt információvagyon bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzésére és fenntartására irányuló intézkedések bevezetésére.

Az IBP alapul szolgál továbbá a jelen politikánál alacsonyabb szintű szabályozási eszközök, kialakítására és bevezetésére. Az információ védelem megvalósítása érdekében tervezni és biztosítani kell azokat az anyagi feltételeket, amelyek lehetővé teszik a megfelelő színvonalú technika, valamint a speciális felkészültséget igénylő személyi feltételek megteremtését és folyamatos fenntartását.

3 AZ IBP HATÁLYA

3.1 Személyi hatálya

A politika személyi hatálya kiterjed a:

- Társaság minden munkatársára,
- Társaság szerződéses viszonyban tevékenykedő partnereire.

3.2 Tárgyi hatálya

A politika tárgyi hatálya kiterjed a Társaság

- szabályzataira,
- irányelveire
- eljárásrendjeire,
- rendszerdokumentációira, és minden egyéb dokumentumára.

3.3 Területi hatálya

A politika területi hatálya kiterjed a tárgyi hatálya alá tartozó informatikai erőforrások üzemelési helyszíneire:

- a Társaság telephelyeire
- a külső szolgáltatók által, a Társaságnak nyújtott szolgáltatásban érintett helyszínekre.

3.4 Időbeli hatálya

A politika az aláírás napját követő első munkanapon lép hatályba, dokumentumba foglalt feladatok és szabályok ezen időponttól alkalmazandók. A politika visszavonásig érvényes.

4 AZ IBP MINŐSÍTÉSE

Az IBP belső nyilvános dokumentum, amelyet bárki megismerhet. Jelen politika személyi hatálya alá tartozóknak a szabályzat előírásait kötelezően ismerniük (a munkaviszony kezdetének napján, de legkésőbb az első munkában töltött napon) és követniük kell.

5 AZ IBP FELÜLVIZSGÁLATA

Az IBP-t évente felül kell vizsgálni. A felülvizsgálat az Informatikai Biztonsági Felelős (továbbiakban: IBF) feladata.

6 AZ IBP SZEREPE, MEGFELELŐSÉGE

Az IBP a szabályozási hierarchia (irányelvek – szabályozások – eljárásrendek – kézikönyvek) legfelsőbb szintjén helyezkedik el és ilyen módon hatással van a teljes szabályozási struktúrára. Az IBP-t a Társaság minden munkatársának ismernie kell, kiemelten azoknak, akik a Társaság informatikai rendszerét használják és üzemeltetik. Az IBP megismerését és tudomásul vételét dokumentálni kell.

A jelen IBP-ben megfogalmazottak összhangban vannak a hazai jogszabályokkal és ajánlásokkal, valamint a nemzetközi IT biztonsági szabványokkal.

7 IBP ALAPELVEK ÉS CÉLKITŰZÉSEK

A Társaság az informatikai biztonság területén az alábbi alapelveket és védelmi célkitűzéseket kívánja következetesen érvényesíteni a jogszabályi követelményeknek megfelelően.

7.1 Célkitűzések

Hitelesség biztosítása a Társaság kezelésében lévő adatok tekintetében.

> Szükséges, hogy minden kétséget kizáróan megállapítható legyen a bekerülő adat forrása és az adat valóságnak való megfelelőssége, valamint annak biztosítása, hogy az előállítás után megőrzi ezen minőségét.

Bizalmasság biztosítása a Társaság által kezelt adatokhoz való hozzáférés tekintetében.

> Érvényesülését elsősorban az informatikai rendszerben történő adathozzáférések és adatkezelés, valamint a Társaság kommunikációja során kell biztosítani.

Sértetlenség biztosítása a Társaság adatkezelése, adatfeldolgozása és kommunikációja során.

> A Társaság által történő adatkezelés során követelmény, hogy pontos és a valóságnak mindenben megfelelő információk kerüljenek a rendszerekben feldolgozásra, és ezen információk sértetlensége az adatkezelés során mindvégig biztosított legyen.

Rendelkezésre állás biztosítása a Társaság által kezelt adatok tekintetében.

> A feldolgozott információ tekintetében követelmény annak visszakereshetősége, használhatósága, amelynek záloga az informatikai rendszerek funkcióinak és elérhetőségének folyamatos biztosítása.

7.2 Alapelvek

A védelem teljes körűségének alapelve

A teljes körűségre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén a következő három dimenzióban kell érvényesíteni:

- az összes rendszerelemre,
- a rendszerek architektúrájának minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az alkalmazások szintjén,
- mind a központi, mind a végponti informatikai eszközökre és környezetükre.

A védelem zártságának alapelve

A zárt védelem akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedések megvalósításra kerültek, és azok szerves egységet alkotnak.

A védelem kockázatarányosságának alapelve

A védelem mértéke és költségei a felmért kockázatokkal arányos legyen. Célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség.

A védelem folytonosságának alapelve

Az informatikai rendszerek bevezetése során kialakított védelmi képességeket a rendszer teljes életciklusa alatt folytonosan biztosítani és fejleszteni kell.

8 Kritikus sikertényezők

A Társaság számára az információbiztonság sikeres megvalósítása során kritikus tényezők a következők:

- a biztonsági szabályozó környezet pontos meghatározása,
- a vezetőség elkötelezettsége;
- a biztonsági követelmények, a kockázatbecslés és a kockázatkezelés megértése és helyes alkalmazása;
- a biztonság hatékony menedzselése valamennyi vezető és alkalmazott felé;
- gondoskodás a kellő oktatásról és képzésről;
- átfogó, mindenre kiterjedő és kiegyensúlyozott mérési módszer alkalmazása az információ biztonságmenedzselés teljesítőképességének értékeléséhez és a helyesbítési javaslatok visszacsatolásához.

9 Kockázatalapú megközelítés

A Társaság célul tűzte ki – a kockázatokkal arányos védelem biztosítása érdekében – kockázatelemzés rendszeres végrehajtását (a rendelkezésre álló erőforrások és lehetőségek szerint). A kockázatelemzés ki kell terjedjen a fenyegetések, a gyenge pontok, a nem elviselhető kockázatú tényezők meghatározására, valamint az ezek alapján kialakítandó védelmi intézkedésekre.

10 Szervezeti és felelősségi kérdések

Az IBP-ben lefektetett elvek kidolgozásának és betartatásának minden esetben kell, hogy legyen felelőse, aki jelenleg az IBF. Az IBF közvetlen az Ügyvezető alá rendelt pozíció kell, hogy legyen. Az IBP elvek betartásának helyzetéről az IBF rendszeresen beszámol az Ügyvezetőnek, aki az információ biztonsági feladatok megvalósításának feltételeit biztosítja.

Az IBF joga és kötelessége az információs rendszert érintő változásokat, fejlesztéseket, beruházásokat információbiztonsági szempontból értékelni. Az IBF javaslatok, döntés előkészítő anyagok kidolgozásával segíti az

Ügyvezetőt az információbiztonságot érintő határozatok meghozatalában, a meghozott intézkedéseket érvényesíti, azok hatásfokát folyamatosan méri és értékeli az Ügyvezető által kitűzött célok teljesülése érdekében.

Az IBP betartása minden munkatárs feladata és annak be nem tartása szigorú szankciókat von maga után.

11 Logikai biztonság

A logikai biztonság területén a Társaság vezetésének célkitűzései az alábbiak:

- informatikai rendszerek védelmének megteremtése, hogy megakadályozza a jogosulatlan hozzáféréseket,
- az informatikai rendszerekhez és alkalmazásokhoz való hozzáférési jogok engedélyezésének hivatalos eljárások keretében történő szabályozása,
- információ, illetve adatvagyon megfelelő védelmi szintjének kialakítása, valamint az információ osztályozása,
- rosszindulatú szoftverek - számítógépvírusok, a hálózati férgek, a trójai falovak és a logikai bombák - elleni védekezés hatékony kialakítása, valamint az Internet használat és elektronikus levelezés létesítése és üzemeltetése vonatkozásában megfelelő tűzfalas védelmet kialakítása a külső támadások, illetve a belső erőforrásokhoz történő jogtalan külső hozzáférések megakadályozása érdekében,
- biztonsági követelmények érvényesítése minden, a Társaság külső informatikai adat-, vagy számítástechnikai kapcsolatában, az ennek kialakítására irányuló szerződésekben, vagy megállapodásokban,
- jogosulatlan tevékenységek észlelésének megteremtése,
- informatikai biztonság megteremtése a mobil számítástechnikai és a távmunka végzési eszközök használata esetén. A megkívánt biztonság legyen összemérhető azzal a kockázattal, amelyet az ilyen munkavégzési mód hordoz,
- rendkívüli események kezelésére történő felkészülés,
- alaptevékenységek megszakadásainak leküzdése, és a kritikus szolgálati folyamatok megvédése a nagyobb meghibásodások és a katasztrófák hatásaitól.

12 Fizikai és szervezeti biztonság

A fizikai és szervezeti biztonság területén a Társaság vezetésének célkitűzései az alábbiak:

- a Társaság objektumainak, szervezetének biztonságának szavatolása,
- információ kezelését, feldolgozását végző helyiségek, valamint az egyes eszközök, az abban elhelyezett adattárolók és adathordozók fizikai védelmének biztosítása,
- papíros formában, valamint elektronikusan kezelt és tárolt információk, tárgyi eszközök, vagy szolgálatot teljesítő személyek védelmének biztosítása a különböző eseményektől, mint tűz, víz, áramellátás kimaradása, külső támadások, betörés,
- informatikai, vagy egyéb úton keletkezett adatok és információk kezelése során az előírt fizikai informatikai biztonsági követelmények betartásának elősegítése,
- személyi felelősségek egyértelmű meghatározása és elhatárolása.

13 Adminisztratív biztonság

Az adminisztratív biztonság területén a Társaság vezetésének célkitűzései az alábbiak:

- a Társaság folyamatos, zavartalan és hatékony működését biztosító informatikai szabályozó környezet, illetve feltételrendszer megteremtése,
- teljes körű szabályozó környezet kialakítása, amely kiterjed a koncepciókra, szabályzatokra és eljárásrendekre.
- A Társaság kiemelt figyelmet fordít a felhasznált szoftverek jogtisztaságára, mindent megtesz a jogtiszta szoftver használat érdekében és az illegális használat, illetve másolás ellen.

14 Biztonsági incidensek kezelése

A Társaság olyan eljárásokat és belső folyamatokat alakít ki, amelyek lehetővé teszik az esetlegesen bekövetkező biztonsági események észlelését, továbbá az irányítási rendszerben olyan belső szabályzókat hoz létre, amelyekkel biztosítottá válik a biztonsági események hatékony és gyors kezelése.

15 Az információ biztonság ellenőrzése, fenntartása

Az IBP által megkövetelt információ biztonsági rendszer fenntartása alapvetően fontos stratégia cél. Ennek felelőse az IBF. Az IBF által elvégzendő távlati feladatokat a Társaság stratégiája, az IBF rendszeres feladatait pedig az IBSz tartalmazza. A stratégiában elhatározott és az IBSz-ben előírt feladatok végrehajtásához szükséges feltételek biztosításáért az Ügyvezető felel. Az informatikai biztonság megfelelő és eredményes működésének és folyamatos fejlesztésének érdekében az IBF rendszeres felülvizsgálatokat hajt végre. A Társaság informatikai biztonságának fenntartásához elengedhetetlenül szükséges a munkatársak biztonságtudatosságának fejlesztése és fenntartása. Ennek érdekében az oktatási tervben szerepeltetni kell a munkatársak évenkénti biztonsági oktatását.

16 Biztonságtudatosság, etika, oktatás

A Társaság vezetése fel kívánja hívni minden – a jelen dokumentum szervezeti hatálya alá tartozó – személy figyelmét arra, hogy az informatikai biztonság sikeres működtetéséhez elengedhetetlen a biztonságtudatos, felelősségteljes magatartás. Tekintettel arra, hogy minden biztonsági rendszer olyan erős, mint a rendszer leggyengébb láncszeme, a Társaság vezetése elvárja mindenkitől, hogy napi tevékenységét a szabályzatok figyelembevételével végezze, senki ne adjon módot arra, hogy a Társaság rajta keresztül támadhatóvá váljék, vagy esetleg önmaga támadóként lépjen fel.

A Társaság vezetése elvárja mindenkitől, hogy az informatikai biztonsággal kapcsolatos szabályokon túl azok szellemiségével összhangban tevékenykedjen, és vegye figyelembe azt, hogy amely cselekedet nincs tiltva, az nem jelenti azt, hogy az a cselekedet etikus. Annak érdekében, hogy az informatikai biztonság mindenki számára érthető és betartható legyen, a Társaság rendszeresen információbiztonsági oktatást szervez, amelyen a megjelenés kötelező. Az oktatások célja, hogy:

- mindenki alapismereteket szerezzen az információbiztonsággal kapcsolatban,
- az informatikai biztonsági rendszerben bekövetkezett változásokról mindenki értesüljön,
- az időközben feltárt biztonsági események kiértékelésével mindenki átérezze az információvédelem szükségességét.

17 Hatályon kívül helyezés

Nincs hatályon kívül helyezendő dokumentum.

18 Mellékletek és formanyomtatványok

Nincsenek mellékletek és formanyomtatványok

19 MÓDOSÍTÁS NYILVÁNTARTÓ-LAP

Módosítások		
Száma	Dátuma	Leírása (jellege)
1	2022. december 09.	Eredeti verzió