TopNet Magyarország Kft.

INFORMATIKAI BIZTONSÁGI POLITIKÁJA

Web: www.topnetmo.hu
E-mail: info@topnetmo.hu
Cím: 6326 Harta, Templom. u. 113.
Telefon: +36-78/400-000
FAX: +36-78/507-570
Iroda:6326 Harta, Templom u. 113.

Tartalomjegyzék

1 BEVEZETÉS

A szervezet tevékenysége során igénybe vett és a közben keletkező információk, továbbá a normál napi ügyvitelt, és az adatfeldolgozást támogató informatikai és kommunikációs eszközök jelentős üzleti vagyont képviselhetnek. Bizalmas mivoltuk, megbízhatóságuk, és a hozzáférhetőségük minősége alapvető jelentőséggel bír, a szervezet versenyképességének és a jövedelem termelő magatartásának megőrzésében, a releváns jogszabályoknak való megfelelősségnek, de akár jó hírének fenntartásában is.

1.1 Az Informatikai Biztonsági Politika célja

A TopNet Magyarország Kft. (a továbbiakban: Cég, vállalkozás) Informatikai Biztonsági Stratégiájának (a továbbiakban: IBP) célja, hogy a vonatkozó jogszabályoknak megfelelően, figyelembe véve a Cég belső szabályozó környezetét, meghatározza azokat a követendő alapelveket, melyek az informatikai és kommunikációs rendszerek által kezelt információs vagyon bizalmassága, sértetlensége, rendelkezésre állásának biztosítása és funkcionalitása, továbbá üzembiztonsága fenntartása érdekében vonatkoznak.

1.1.1 Az információ biztonság keret rendszere

Az információ biztonság keret rendszere, a vállalkozás tevékenységének elvárt szintű fenntartásának biztosításával, és annak biztonságos működését veszélyeztető események megelőzésével, továbbá negatív hatásának minimalizálásával foglalkozik.
Ezért cél az, hogy egy olyan kontrolrendszer kerüljön kialakításra, bevezetésre és működtetésre, amely fenntartja a vállalkozás folyamatos, elvárt szintű üzleti tevékenységét, és minimalizálja a működés során felmerült negatív kihatású biztonsági eseményeket.

1.1.2 Az információ biztonság aspektusai

A vállalkozás tevékenysége során keletkező információ is vagyonként jelenik meg, és ennek érdekében meg kell tenni azokat a szükséges intézkedéseket, melyek védenek a jogosulatlan elérés, módosítás és megsemmisülés ellen.
Az információ biztonságának három főbb aspektusa van, amelyek a

- **Bizalmasság**, a kezelt információhoz csak az arra felhatalmazott személyek részére legyen elérhető, továbbá az értékes és érzékeny információk megóvásának biztosítása az illetéktelen hozzáféréstől, illetve annak nyilvánosságra hozatalától;
- **Sértetlenség**, az információ pontosságának, a valóságnak mindenben megfelelő megvédése;

- **Rendelkezésre állás**, az információ szempontjából annak biztosítása, hogy a kezelt rendszerek funkciója, elérhetősége, és az adatok visszakereshetősége megvalósuljon.

A gondosan megfogalmazott informatikai biztonsági alapkövetelmények, a vállalkozás számára fontos információk, rendszerek és szolgáltatások rendelkezésre állásának sérülése, az adatokkal való visszaélések, illetve a vállalkozás folyamatos üzleti tevékenységében történő fennakadás kockázatainak csökkentésére irányulnak.

1.2 Jóváhagyás

Az informatikai biztonsági politikát - összhangban a vállalkozás egyéb céljaival - a vállalkozás vezetősége hagyja jóvá, és hirdetni ki az érintettek számára.

1.3 Az Informatikai Biztonsági Politika felülvizsgálta

Az IBP-t igény szerint legalább két évente, vagy időközben felmerülő jelentősebb infrastrukturális, továbbá egyéb releváns változás esetén felül kell vizsgálni, és szükség esetén módosítani kell, mind a vállalkozói, mind informatikai szakmai szempontok alapján.

1.4 Az Informatikai Biztonsági Politika értékelése

Rendszeresen meghatározott időközönként értékelni szükséges, hogy a politikában meghatározott elvek hogyan valósulnak meg.

1.5 Az Informatikai Biztonsági Stratégia hatálya

A vállalkozás gondoskodik arról, hogy

- az IBP jogosulatlanok számára ne legyen megismerhető, módosítható, továbbá
- az IBP-ben foglaltak az érintettek részére ismerté váljon.

1.5.1 Az IBP alanyi hatálya

Az IBP alanyi hatálya kiterjed a Cég valamennyi teljes vagy részmunkaidős, továbbá szerződéses munkavállalójára.

1.5.2 Az IBP tárgyi hatálya

Az IBP tárgyi hatálya kiterjed a Cég informatikai rendszerének üzemeltetésében, fejlesztésében és karbantartásában résztvevő cégekre, illetve azon magánszemélyekre, akik közvetve, vagy közvetlenül kapcsolódnak a vállalkozáshoz, fizikai elhelyezkedéstől, illetve a tulajdonos, vagy üzemeltető személyétől függetlenül.

1.5.3 Az IBP időbeli hatálya

Az IBP időbeli hatálya visszavonásig érvényes.

1.6 Informatikai biztonsági felelős

Az informatikai biztonsági feladatok elvégzésére a vállalat vezetőségének ki kell jelölni egy Informatikai Biztonsági Felelőst.

1.7 Vezetőségi elkötelezettség

A vállalat vezetősége számára kiemelt fontossággal bír az informatikai biztonsági keretrendszer működtetése, és elvárja minden érintett személy részéről a politika irányelveinek, és az ehhez kapcsolódó szabályok betartását!

1.8 Kapcsolódó dokumentumok

- Informatikai Biztonsági Stratégia
- Informatikai Biztonsági Szabályzat

2 KOCKÁZAT ELEMZÉS ALAPELVEI

A kockázatelemzés során ajánlott figyelembe venni a releváns nemzetközi vagy hazai szabványokat, ajánlásokat, legjobb gyakorlatokat. Informatikai biztonsági szempontból, a kockázatelemzés alapját képezi az adatok és informatikai rendszerelemek bizalmasságának, sértetlenségének és rendelkezésre állásának, és ezek sérüléséből, elvesztéséből bekövetkező káros hatás nagysága, terjedelme, továbbá a káros hatás bekövetkezésének veszélyes mértéke, becsült valószínűsége.

3 OSZTÁLYBA SOROLÁS ALAPELVEI

A biztonsági osztályba sorolás - összhangban a releváns jogszabályokkal -, a kezelt adatok minősége és az informatikai rendszerelemek által kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának sérülése esetén potenciálisan bekövetkező káresemény nagyságának és a rendelkezésre álló erőforrások figyelembe vétele alapján történik meg.
Az osztályba sorolás közben, az elvárttól eltérő hiányosságok kiküszöbölésére Intézkedési Tervet kell készíteni.

4 AZ INFORMATIKAI BIZTONSÁG ALAPELVEI

Az informatikai keretrendszer kialakításakor olyan fizikai-, logikai és adminisztratív irányelveket kell megfogalmazni, ami összhangban van szervezet működésével és a releváns jogszabályokkal.

4.1 A kockázatarányos védelem elve

Az informatikai biztonsági intézkedéseket úgy kell meghatározni, hogy annak költség vonzata arányban álljon a haszon megtérüléssel. Az intézkedéseket kockázat arányosan kell mérlegelni, melyeket rendszeresen felül kell vizsgálni. A maradvány kockázatokat a vezetőségnek dokumentáltan el kell fogadnia.

4.2 Teljes körű védelem elve

Az informatikai biztonsági intézkedéseket a vállalkozás minden elemére érvényre kell juttatni.

4.3 Az egyenszilárdság elve

Az egyenszilárdság elve szerint, azonos erősségű biztonsági szintek kerüljenek kialakításra minden egyes biztonsági rendszer kialakításkor.

4.4 Rendszerfejlesztések biztonsági elv

Az alkalmazások és szolgáltatások fejlesztési életciklusa során a biztonság tudatosság, mint

követelmény jelen kell, hogy legyen, a tervezésétől kezdődve egészen a bevezetésig.

4.5 A „négy szem” elv

A vállalkozás működése során, annak kritikus folyamataiba felülvizsgálatokat kell beiktatni úgy, hogy a folyamat csak akkor tudjon tovább lépni, ha azt legalább két személy ellenőrizte. Szúró próbaszerűen a vezeti is gyakorolhat ellenőrzési tevékenységet.

4.6 A szükséges és elégséges hozzáférés elve

A vállalkozás rendszereihez és helyiségeihez való hozzáférések szintjét úgy kell meghatározni, hogy az igénybe vevő csak a munkája elvégzéshez szükséges jogokat kapja meg, és ne többet.

4.7 Fizikai biztonság

A fizikai biztonság kialakításakor cél az illetéktelen hozzáférés megakadályozása. Az informatikai rendszerek külső környezeti hatásoktól való védelmét úgy kell kialakítani, hogy a vállalkozás értékei, eszközei, és a szolgáltatás folytonossága ne legyen fenyegetve.

4.8 Vírusvédelem

A rosszindulatú, kártékony alkalmazások ellen naprakész védelmi rendszerrel kell rendelkezni. A felhasználókat oktatásban kell részesíteni, illetve fel kell készíteni őket a megelőző és elkerülő magatartásra.

4.9 Mentés, archiválás

A törvényi kötelezettségeknek megfelelő mentési, archiválási rendszert úgy kell kialakítani, hogy elvárt feltételek mellett lehetőség legyen az információk visszaállítása. Nem várt esemény bekövetkeztekor, a rendszer, illetve a kezelt adatok visszaállíthatók egy korábbi időpontra, ezzel is csökkentve a kár mértékét.

4.10 Naplózás

Az informatikai rendszer használatát a telepített, illetve beépített lehetőségek (pl. naplózás bekapcsolása) segítségével nyomon kell követni, és gondoskodni kell annak ellenőrzéséről is.

4.11 Incidensek kezelése

A napi normál üzletszerű működés során felmerült informatikai biztonsági fenyegetéseket haladéktalanul jeleneti kell az Informatikai Biztonsági Felelősnek.

4.12 Működésfolytonosság fenntartása

Meg kell határozni azokat a fő irányelveket és módszereket, melyek segítségével biztosíthatók a kritikus folyamatok, szolgáltatások folytonossága fenntartható nem várt esemény bekövetkeztekor.

4.13 Oktatás, képzés, - a biztonságtudatosság fokozása

A biztonságtudatosság növelése érdekében oktatásokat, képzéseket kell tartani.