Kivonat az MVM MÁTRA MÉLYÉPÍTŐ KFT. MVMM-SZ028/2021. számú

INFOKOMMUNIKÁCIÓS SZABÁLYZAT-ából

1. A SZABÁLYOZÁS CÉLJA

Jelen Infokommunikációs Szabályzat (továbbiakban: Szabályzat) funkcionális célja az MVM Mátra Mélyépítő Kft.-nél (továbbiakban: Társaság):

- egységes szemléletben meghatározni a felhasználók és az információtechnológiai rendszerek viszonyát az informatikai rendszerek által kezelt adatok, információk bizalmasságának, sértetlenségének, rendelkezésre állásának megőrzése érdekében;
- a Társaság ügyviteli működési környezetébe kerülő, illetve ott keletkező adatok, információk informatikai rendszere(ke)n történő adatfeldolgozásával szemben támasztott biztonsági követelmények rögzítése;
- az informatikai, valamint kommunikációs berendezések (hardver) és alkalmazott rendszerek (szoftver) biztonságának elősegítése;
- a felhasználók által a számítástechnikai eszközök, hálózatok, rendszerek, szoftverek és az internet felhasználása során alkalmazandó biztonsági követelményrendszer meghatározása,
- azon alapvető biztonsági normák és működési keretek meghatározása, amelyek érvényesítésével a Társaság az elfogadható minimumra csökkentheti az információkezelés nem kívánt (működésre negatív hatást kifejtő) következményeit;
- az adatbiztonsággal kapcsolatos szerepek, feladat- és felelősségi körök rögzítése;

A Szabályzat rendelkezéseit minden üzemszerűen használt ügyviteli rendszer és munkafolyamat esetében teljeskörűen, a releváns kockázatokkal arányos módon szükséges alkalmazni.

2. A SZABÁLYZAT HATÁLYA

2.1. Időbeli hatály

Jelen szabályzat 2024. április 30. napjától a hatályon kívül helyezésig alkalmazandó. Jelen szabályzat mellékletei és formanyomtatványai a szabályzat egységes, elválaszthatatlan részét képezik.

2.2. Személyi hatály

A Szabályzat személyi hatálya kiterjed:

- a MVM Mátra Mélyépítő Kft. valamennyi szervezeti egységére és munkavállalójára, akik informatikai és/vagy telekommunikációs eszközt használnak;
- a MVM Mátra Mélyépítő Kft. által igénybe vett ügyviteli informatikai rendszerekkel, szolgáltatásokkal összefüggésben, a Társasággal szerződéses jogviszonyba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban: külső személy), a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben;
- a MVM Mátra Mélyépítő Kft. által igénybe vett IT rendszereket használó, a rendszerekhez és alkalmazásokhoz bármilyen hozzáféréssel rendelkező természetes vagy jogi személyre, a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben.

Jelen szabályzatot, illetve annak kivonatát ismertetni kell minden, a személyi hatálya alá tartozó féllel, a szabályzatban foglaltak megismeréséről és betartásáról az érintett feleknek írásban nyilatkoznia kell (1. és 2. formanyomtatvány).

2.3. Tárgyi hatály

A szabályzat hatálya kiterjed a MVM Mátra Mélyépítő Kft. tulajdonában vagy használatában lévő informatikai rendszerekben előforduló adatokra, információkra, a MVM Mátra Mélyépítő Kft. tulajdonában vagy használatában lévő informatikai rendszerek teljes életciklusára (tervezés, fejlesztés, beszerzés, bevezetés, üzemeltetés, kivonás).

Ügyviteli informatikai eszközök (IT)

A Kivonat tárgyi hatóköre az alábbiakba felsorolt ügyviteli informatikai eszközökre terjed ki. Az ügyviteli az informatikai rendszereket a megbízott informatikus üzemelteti. A hatókörbe tartozó Ügyviteli informatikai eszközök:

- munkaállomások,
- szerverek,
- hálózati eszközök,
- multifunkciós másoló-nyomtatók-szkennerek, nyomtatók,
- egyéb IT eszközök,
- okoseszközök (okostelefonok, tabletek, PDA-k stb.),
- külső hordozható adattároló eszközök.

2.4. Fizikai biztonság

2.4.1. Területek védelme, biztosítása

A Társaság területén kamerarendszer működik.

2.4.2. Irodák, helyiségek és egyéb létesítmények védelme

A társaság helyiségei a fizikai és környezeti biztonság szempontjából az alábbi biztonsági zónába sorolhatóak:

Nyilvános területek

A társaság mindazon területei, helyiségei, amelyek látogatók számára nyilvánosak, ugyanakkor a társaság szempontjából magánterületnek minősülnek. Ilyen a recepció és az ügyfélváró, továbbá a vendég mellékhelyiség.

Irodai terület kategória

Csak a társaság munkavállalói, külső partnerek – külön engedély alapján – belépésre jogosult munkavállalói, illetve vendégek csak kísérettel léphetnek be. Ilyen a nyílt irodai tér, a tárgyalók és projektszoba helyiségek.

Fokozottan védett kategória

Fokozottan védett helyiségnek kell tekinteni azokat a helyiségeket, ahol bizalmas adatok feldolgozására, tárolására alkalmazott kiegészítő informatikai erőforrások találhatók, valamint ide sorolandók a felsővezetői irodák, helyiségek. Az ide tartozó helyiségeket zárható ajtóval kell ellátni.

Fokozottan védett kategóriába a következő helyiségeket kell sorolni:

- az aktív hálózati elemek elhelyezésére és üzemelésére szolgáló helyiségek, szekrények;
- használaton kívüli, adathordozót tartalmazó IT eszközök tárolására szolgáló helyiségek;

- ügyvezető igazgatói iroda, valamint a biztonsági terület tevékenysége során keletkező dokumentumok (adathordozók, nyomtatványok stb.) és technikai eszközök tárolására kijelölt helyiség.

Kiemelten védett kategória

Kiemelten védett helyiségnek kell tekinteni azokat a helyiségeket, ahol bizalmas adatok feldolgozására, tárolására alkalmazott központi informatikai erőforrások találhatók.
Kiemelten védett (zárt) helyiségekbe csak ellenőrzött módon és csak az arra jogosult személyek juthatnak be. A bejutás és benntartózkodás során kíséretet kell biztosítani a külső személyek részére.
Ebbe a kategóriába az alábbi helyiségek tartoznak:

- Vagyonvédelmi és központi kiszolgáló informatikai eszközök elhelyezésére használt helyiség (továbbiakban: szerverszoba).

Az informatikai rendszerek fejlesztése kapcsán külön szükséges kezelni az ügyviteli és a technológiai rendszereket.
Informatikai rendszerek fejlesztése tekintetében a használt alkalmazásoknak két típusát különböztetjük meg:

- **Belső fejlesztésű** rendszerek: A társaság által fejlesztett ügyviteli vagy technológiai alkalmazások.
- **Külső fejlesztésű** rendszerek: Nem a társaság által fejlesztett alkalmazások, olyan ügyviteli vagy technológiai informatikai rendszerek vagy rendszerelemek, melyeket a társaság külső szolgáltatótól vesz igénybe, közvetlenül vagy az informatikai szolgáltatón keresztül. Ezen belül három alkategória különböztethető meg:
  - Dedikáltan a társaság számára fejlesztett alkalmazás, melyet más személy vagy vállalat nem használhat.
  - Általános funkciókat ellátó, bárki számára elérhető alkalmazás („dobozos" termék).
  - Felhő alapú szolgáltatás.

  A külső fejlesztésű rendszerek szerződése tartalmazza a telepítési és használati feltételeket, valamint a fejlesztési lehetőségeket, verziókövetést. Ebben az esetben a fejlesztővel/szállítóval kötött szerződésben kell kitérni az IT biztonsági követelményekre, melyet a Társaság IT biztonsági szakértője ellenőriz.

2.4.3. Általános irányelvek informatikai rendszerek fejlesztésére, beszerzésére vonatkozóan

Az informatikai rendszerek fejlesztését a következő IT biztonsági követelmények szerint kell végrehajtani.

Igények azonosítása

Az új igény egyeztetése során be kell vonni a Társaság IT biztonsági szakértőjét az új rendszerrel vagy fejlesztéssel kapcsolatos kockázatok korai feltárása végett. Az információbiztonsági szempontú véleményezésnek, jóváhagyásnak minden esetben dokumentált módon kell megtörténnie.

Fejlesztési terv készítése és jóváhagyása

A fejlesztési terv elkészítésénél minden esetben figyelembe kell venni az IT biztonsági követelmények biztosítását, meghatározni az információbiztonsági kockázatokat, ezért a dokumentum összeállításába a Társaság IT biztonsági szakértőjét is be kell vonni. Az IT biztonsági szakértő bevonásának elmaradásából származó károkért a fejlesztési projekt vezetője felelős.
Fejlesztés csak abban az esetben kerülhet megkezdésre, amennyiben az ügyvezető igazgató jóváhagyta a fejlesztési tervet.

Fejlesztés megvalósítása

Belső fejlesztés esetén az informatikai szolgáltatónak vagy a fejlesztésben érintett társaságnak vagy a Társaságunk fejlesztésben érintett szervezeti egységének fejlesztési módszertannal/szabályzattal kell rendelkeznie, mely dokumentálja a fejlesztések megvalósításának menetét, szabályait, kitérve az IT biztonsági követelményekre.

Külső fejlesztésű rendszerek esetén a beszerzés előírásait kell figyelembe venni, továbbá a beszerzési kiírásba és eljárásba be kell vonni az IT biztonsági szakértőt. (illetve minden, a fejlesztésben közvetlenül érintett társaságok IT biztonsági felelőseit), aki azonosítja az IT biztonsági kockázatokat, azok kezelését, valamint meghatározza a fejlesztő számára előzetesen kiadható információkat és azok kiadásának feltételeit.

Felhő alapú rendszerek igénybevételének igénye esetén a rendszer bevezetése előtt az IT biztonsági szakértőnek ellenőriznie kell a szolgáltató IT biztonsági megoldásainak megfelelőségét (interjú vagy dokumentum vizsgálat). Ajánlása alapján az ügyvezető igazgató hagyja jóvá a rendszerben tárolt/kezelt adatok körét, figyelembe véve az adatok besorolását. Az ellenőrzés eredményét dokumentált módon rögzíteni kell, a dokumentáció tárolása az IT biztonsági szakértő feladata. Bizalmas adat csak maszkolva, illetve megfelelő titkosítás mellett kerülhet fel a felhő alapú alkalmazásba, szigorúan bizalmas adatok felhőben való tárolása nem engedélyezett.

2.5. Külső közreműködők, harmadik fél hozzáférése

Belső használatú, illetve annál magasabb minősítésű adatot külső (harmadik) félnek továbbítani, vagy ahhoz hozzáférést biztosítani csak jogszabályi kötelezettség, illetve szerződéses kapcsolat vagy a társaság első számú vezetőjének meghatalmazása alapján lehet, kizárólag az adott feladattal összefüggésben, az ahhoz szükséges mértékben, formában és tartalomban, a megfelelő jogosultság és felhatalmazás alapján, az abban meghatározott időtartam alatt. A harmadik fél jogosultságáról, illetve az adatok, információk kezeléséhez szükséges feltételek rendelkezésre állásáról (pl. titoktartási nyilatkozat) a továbbítás/betekintés lehetővé tétele előtt meg kell győződni.

Az információbiztonsági szabályozás szempontjából külső közreműködőnek/harmadik félnek minősülnek a társaság alvállalkozói, szerződéses partnerei, valamint a társasági domain-be nem tartozó társaságok, a hatóságok, valamint a média.

2.5.1. Külső felek közreműködésével kapcsolatos általános szabályok

- Szerződéses partnerek esetében (a továbbiakban ide értendő a társasági első számú vezető általi meghatalmazással rendelkezők) a szerződésnek tartalmaznia kell a szerződéses jogviszony alatt fennálló IT biztonsági követelményeket, azok megszegéséből származó szankciókat is. A szerződés IT biztonság szempontból történő jóváhagyása az ügyvezető igazgató hatáskörébe tartozik.
    - Elektronikus dokumentumok átadásánál az Elektronikus kommunikáció című fejezetben rögzített titkosítási eljárást kell követni az elektronikus levelezés során, illetve nagy mennyiségű adat átadása esetén preferálni kell a titkosított adathordozók használatát.

- A szerződéses partnernek lehetővé kell tennie a biztonságtudatos munkavégzés feltételeinek megteremtését, továbbá a munkakör ellátásához szükséges, megfelelő biztonsági feltételekkel rendelkező eszközök biztosítását. Amennyiben a szerződéses partner a rögzített feltételek teljesítését nem tudja garantálni, vagy az átadott adatok biztonsági besorolása megköveteli, a társaság a munkavégzés idejére munkaállomást és/vagy projektszobát biztosíthat.

- Az IT biztonsági követelmények betartását a társaság keretein belül a társaság IT biztonsági szakértője ellenőrzi.
- Az ellenőrzésekről jelentést kell készíteni, melyet mind a harmadik fél képviselője, mind az adott vállalkozóért felelős terület vezetője felé meg kell küldeni. Súlyos, vagy folyamatosan fennálló nem-megfelelőség vagy hiányosság azonosítása esetén tájékoztatni kell az ügyvezető igazgatót is.

2.5.2. Adatok átadása harmadik félnek

Adatok átadása harmadik félnek csak az 5.16.1. fejezetben rögzített feltételek teljesítését követően, a szerződésben meghatározott módon lehetséges.

Papír alapú dokumentumok átadása esetén törekedni kell a személyes átadásra, továbbá a dokumentum továbbításakor figyelembe kell venni az 5.4. fejezetben, rögzített követelményeket.

Elektronikus dokumentumok átadásánál az 5.11. fejezetben rögzített titkosítási eljárást kell követni az elektronikus levelezés során, illetve nagy mennyiségű adat átadása esetén preferálni kell a titkosított adathordozók használatát.

A szerződéses partnernek lehetővé kell tennie a biztonságtudatos munkavégzés feltételeinek megteremtését, továbbá a munkakör ellátásához szükséges, megfelelő biztonsági feltételekkel rendelkező eszközök biztosítását. Amennyiben a szerződéses partner a rögzített feltételek teljesítését nem tudja garantálni, vagy az átadott adatok biztonsági minősítése megköveteli, a társaság a munkavégzés idejére munkaállomást és/vagy projektszobát biztosíthat.

Az adatok előírásoknak megfelelően történő átadása mind a társaság, mind a szerződött külső fél felelőssége. A nem-megfelelő adatátadásból származó károkért az érintett felhasználók a társasági és a szerződött partneri oldalon egyaránt szankcionálhatók az 5.6.5. pontban meghatározottak szerint.

2.5.3. Ideiglenes belépési jogosultság adása harmadik félnek

Amennyiben a szerződött külső féllel való munka indokolja (pl. projekt időtartama, intenzitása), külső szereplők számára belépőkártya az MVMM-SZ002/2021 Személy- és gépjármű forgalom beléptetési rendje eljárásrend előírásai alapján adható ki.

2.5.4. Hozzáférési jogosultság biztosítása informatikai rendszerhez

Nem az MVM Mátra Mélyépítő Kft. által biztosított számítógépek a társasági hálózatra nem csatlakoztathatók, így a külső partner által hozott, az ő tulajdonát képező számítógép sem. Ezen

eszközök esetében előzetes egyeztetés és az ügyvezető igazgató engedélye alapján vendég WiFi hozzáférés kérhető.
Amennyiben a külső félnek átadandó, vagy általa létrehozandó adatok biztonságos megosztása nem lehetséges, vagy azok külső eszközön történő kezelése nem engedélyezett, lehetőség van a külső fél munkatársainak hordozható adattároló, illetve munkaállomás és a szükséges informatikai rendszerekhez jogosultság igénylésére.
A külső partnernek a társaság informatikai rendszeréhez adott felhasználói azonosítók csak azokhoz az információkhoz és olyan mértékben adhatnak hozzáférést és jogosultsági szintet, amennyi az együttműködés során a munkavégzéshez feltétlen szükséges. Harmadik fél hozzáférési jogosultságáról az ügyvezető igazgató dönt.
Minden harmadik félnek a hozzáférési jogosultság kiadása előtt meg kell ismernie jelen szabályzatot és írásban nyilatkozni kell (2. sz. formanyomtatvány) az abban foglaltak elfogadásáról és titoktartási kötelezettség vállalásáról.
A harmadik fél hozzáférési jogosultságait csak arra az időtartamra szabad kiadni, amelyre a harmadik fél szerződése vonatkozik, de legkésőbb tárgyév végéig. Ennek érdekében, amely rendszernél lehetséges, automatikus lejáratot kell beállítani, illetve a szerződés megszűnésével egyidejűleg, azonnal vissza kell vonni a kiadott jogosultságokat.
A hozzáférési jogosultság megújításáért a fogadó fél felel, év végi törlését az ügyvezető igazgató utasítása alapján a megbízott informatikus végrehajtja.
Külső szereplőknek hordozható informatikai eszköz (laptop, USB adattároló, VPN hardverkulcs stb.) akkor adható, ha ez szerepel a szerződésben, és az eszközzel elszámolási kötelezettsége van, de preferált a helyi, asztali munkaállomások használata.
Külső szereplők nem szerezhetnek a társaság számítógépes hálózatán semmilyen privilegizált (pl. adminisztrátori) jogosultságokat, kivéve amennyiben informatikai rendszer üzemeltetése az alvállalkozói együttműködés tárgya. Ebben az esetben a kiemelt jogosultságot dokumentálni kell, illetve a kiemelt jogosultság csak az aktuális munkavégzés időtartamára adható ki. A szerződésben részletesen szükséges továbbá annak szabályozása, hogy a külső partner rendszergazdai jogai mire jogosítják fel, továbbá ezek kontrollja és monitoringja hogyan történik.
A külső szereplőknek az informatikai rendszerhez adott felhasználói azonosítók nyilvántartása legyen naprakész, kontrollja és monitorozása folyamatos kell, hogy legyen – ezek nyilvántartása a megbízott informatikus feladata.
A társaság által biztosított eszközökön, illetve a társaság területén a társasági információbiztonsági szabályzatban rögzített biztonsági előírások betartása kötelező.
Azok az adatok, információk, dokumentumok, amelyek szigorúan bizalmas kategóriába tartoznak, adathordozón vagy nyomtatott formában sem adhatók ki, még titoktartási nyilatkozat aláírása mellett sem. Ebben az esetben, amennyiben indokolt, a betekintést adatszobán/projektszobán keresztül kell biztosítani.

2.5.5. Projektszoba, adatszoba

Projektszoba, adatszoba kialakítására abban az esetben van szükség, amennyiben a külső félnek átadandó, vagy általa létrehozandó adatok biztonságos megosztása nem lehetséges, vagy azok külső eszközön történő kezelése nem engedélyezett, vagy a projekt jellegéből, a külső munkatársak létszámából adódóan osztott irodai munkaállomások biztosítása nem elegendő.

A projektszoba kialakításával és működésével kapcsolatos alapvető elvárásokat MVM ajánlás alapján, a társaság IT biztonsági szakértője határozza meg.

2.5.6. Ellenőrzések

Jelen fejezetben rögzített, harmadik félre vonatkozó információbiztonsági, IT biztonsági előírásokat a társaság IT biztonsági szakértője köteles ellenőrizni.

Harmadik féllel kötött szerződésben részletesen dokumentálni kell az ellenőrzés gyakoriságát, a vizsgálat tárgyát, illetve a vizsgálat módját.

Eltérés esetén a hiányosság vagy nem-megfelelőség kezelésére határidőt kell kiszabni, melynek leteltét követően visszaellenőrzést szükséges végezni az érintett pontokon.

Az ellenőrzésekről jelentést kell készíteni, melyet a harmadik fél képviselője és az adott vállalkozóért felelős terület vezetője felé egyaránt meg kell küldeni. Súlyos, vagy folyamatosan fennálló nem-megfelelőség vagy hiányosság azonosítása esetén tájékoztatni kell a felső vezetést is.

2.6. Incidenskezelés

Informatikai biztonsági eseménynek/incidensnek tekinthető minden, az informatikai eszközökkel kapcsolatban felmerülő, hardveres vagy szoftveres meghibásodás, probléma, a megszokottól eltérő, rendellenes működés (pl. vírusfertőzés, adathalász támadás, adathordozó/mobil eszköz elvesztése, jelszó kompromittálódása, stb.). Ide sorolhatók azon események vagy incidensek is, melyek nem sorolhatók be egyértelműen a fizikai biztonsági esemény/incidens kategóriába (pl. bizalmas dokumentumok elvesztése, kompromittálódása, személyes adatok kezelésére vonatkozó szabályok megsértése, stb.).

A Társaság minden munkavállalójának és külső partnerének kötelessége az általa tapasztalt biztonsági eseményt, vagy általa feltárt biztonsági sebezhetőséget haladéktalanul bejelenteni a társaság IT biztonsági szakértőjének.

Visonta, 2024. 10. 28.