Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

Opennetworks Kereskedelmi és Szolgáltató Kft.

Információ Biztonsági Politika

(IBP)

Verzió 6.0.

Jóváhagyta: Beliczay András, ügyvezető

2020. szeptember 10.

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

Tartalomjegyzék

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

1. Dokumentum Karbantartás

Dokumentum változások története

Verzió	Dátum	Változások leírása	Módosítva
1.0	2015-02-02	1. verzió	Stark Judit, IBF
1.1.	2015-03-16	Véglegesen kidolgozott 1. verzió	Beliczay András, ügyvezető
2.0.	2016-03-29.	2016. márciusi éves felülvizsgálat: jogszabályi hivatkozások frissítése	Stark Judit, IBF
3.0	2017-07-10	2017. évi audit előkészítés: jogszabályi hivatkozások frissítése, Informatikai biztonsági tervezés, személybiztonság-tervezés, rendszerbiztonsági terv készítés célkitűzésének megfogalmazása.	Stark Judit, IBF
4.0	2018-08-29	2018. évi éves felülvizsgálat, GDPR kompatibilitás megteremtése	Stark Judit, IBF
5.0	2019-09-03	2019. évi éves felülvizsgálat, jogszabályok, intézkedési terv elhelyezése az IBDR-ben	Stark Judit, IBF
6.0	2020-09-10	2020. évi éves felülvizsgálat – intézkedési tervre vonatkozó pontosítás	Stark Judit, IBF

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

2. Bevezetés, vezetői elkötelezettség

Az információs társadalom üzleti kihívásaira válaszolva az Opennetworks Kereskedelmi és Szolgáltató Kft. (továbbiakban: Opennetworks, Cég) vezetésének szilárd meggyőződése, hogy az általa kezelt adat-, és információvagyont védeni kell a különböző fenyegetettségek ellen, a bizalmasság, a sértetlenség, a rendelkezésre állás, illetve az üzletmenet folytonosság biztosítása érdekében. Az információvagyon védelméről átfogó módon gondoskodik a Cég, a rá vonatkozó jogszabályi kötelezettségeket szem előtt tartva. Az Opennetworks e téren képviselt irányelveit jelen **Információ Biztonsági Politikában (a továbbiakban IBP)** teszi közzé. Az Opennetworks vezetése a jelen IBP-ben meghatározott egyetemleges alapelvek és belső biztonsági alapkövetelmények maradéktalan teljesítését várja el valamennyi munkatársától, beszállítóitól és miden egyéb érdekelt féltől. Az IBP kivétel nélkül kiterjed az Opennetworks által végzett valamennyi folyamatra, alkalmazott rendszerre és a cég valamennyi szervezeti egységére. A vezetés biztosítja az IBP teljesítéséhez szükséges erőforrásokat.

3. Az IBP célja

Az IBP az Opennetworks legfelső vezetésének akaratnyilvánítása a cég informatikai rendszerei által kezelt adat-, és információvagyon bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetésére.

Az IBP alapul szolgál továbbá a biztonsági politikánál alacsonyabb szintű szabályozások kialakításához, a jelen és jövőbeli informatikai biztonsági döntések meghozatalához, illetve a biztonsági rendszer működtetői és a felhasználók számára a napi rendeltetésszerű tevékenységük gyakorlásához.

Az információ védelem megvalósítása érdekében tervezni és biztosítani kell azokat az erőforrásokat, amelyek lehetővé teszik a megfelelő színvonalú technikai, valamint a speciális felkészültséget igénylő személyi feltételek megteremtését és folyamatos fenntartását.

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

4. Az IBP hatálya

4.1. Az IBP személyi hatálya

Az IBP személyi hatálya kiterjed:

a) A Cég minden munkatársára (a rendszerek felhasználóira, fejlesztőire, üzemeltetőire)
b) Azokra a harmadik személyekre, melyek – szerződéses viszonyuk alapján – a Cég által kezelt adatvagyonnal vagy az azt kezelő informatikai rendszerekkel kapcsolatba kerülnek (a rendszerek felhasználóira, fejlesztőire, üzemeltetőire, az adatok adatfeldolgozóira)

A jelen IBP személyi hatálya alá tartozóknak a biztonsági politika célkitűzéseit ismerniük és követniük kell.

4.2. Az IBP tárgyi hatálya

Az IBP tárgyi hatálya kiterjed a Cég által használt valamennyi informatikai rendszerre, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi a keletkező, illetve felhasznált adatokat, információkat.

Ezen belül a felhasznált:

a) hardver eszközökre
b) adathordozókra
c) alap szoftverekre
d) alkalmazásokra
e) az informatikai rendszerek üzemelési környezetét biztosító objektumokra és környezeti infrastruktúra elemekre.

4.3. Az IBP területi hatálya

Az IBP területi hatálya kiterjed a tárgyi hatálya alá tartozó informatikai

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

erőforrások üzemelési és használati helyszíneire:

a) a Cég székhelyére
b) a Cég telephelyeire
c) a mindenkori bérelt helyiségeire
d) kiszervezett üzemeltetési, adatkezelési- és adatfeldolgozási tevékenységeinek külső helyszíneire
e) az otthoni használatra adott eszközeire.

4.4. Az IBP-vel érintett tevékenységek és folyamatok

Az IBP hatálya kiterjed azon tevékenységekre, melyek humán, technológiai, természeti és nemzetvédelmi kockázatok tekintetében a Cég tulajdonában, vagy kezelésében lévő materiális, szolgáltatási, vagy információs- és adatvagyon üzleti értékteremtő képességét, vagyoni értékét, állagát, rendelkezésre állását közvetlenül érintik, vagy befolyásolják.

5. Minősítés, elhelyezkedés a szabályozási hierarchiában, jogszabályi megfelelőség, kommunikáció

5.1. Az IBP minősítése

Az IBP nyilvános dokumentum. Az IBP elérhetőségét az Opennetworks honlapján (www.opennet.hu) biztosítja.

5.2. Az IBP elhelyezkedése

Az IBP a szabályozási hierarchia (irányelvek – szabályozások – eljárásrendek – kézikönyvek) legfelsőbb szintjén helyezkedik el és ilyen módon hatással van a teljes szabályozási struktúrára. Ismerete és betartása a 4.1 fejezetben meghatározott valamennyi személy részére kötelező érvényű. Az IBP és az erre épülő alsóbb szintű szabályzatok kibocsátása, az érintettek körében történő

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

közzététele a Cég ügyvezetőjének, karbantartása és folyamatos felülvizsgálata a Cég Informatikai Biztonsági Felelősének (IBF) feladata.

Az IBF az informatikai rendszerek egészére, illetve a rendszerelemek teljes életciklusára, az informatikai biztonság elviselhető kockázati szinten tartása érdekében kialakítja az Opennetworks informatikai biztonsági dokumentációs rendszerét (IBDR), az alábbi elemekkel:

a) Törvényi előírások és egyéb jogszabályok aktuális gyűjteménye
b) Informatikai Biztonsági Politika
c) Informatikai Biztonsági Szabályzat
d) Kockázatelemzések, biztonsági osztályba sorolás
e) Információ Biztonsági Intézkedési terv – a kockázatelemzés részeként, annak eredményei alapján
f) Alsóbb szintű szabályzatok, eljárásrendek, felhasználói dokumentumok

5.3. Az IBP jogszabályi megfelelősége

A jelen IBP-ben megfogalmazottak megfelelnek az érvényes magyar jogszabályoknak, melyek közül az aktuális vonatkozó jogszabályok hivatkozását az IBDR-en belül jelen IBP tartalmazza az alábbiak szerint:

a) 2003. évi C. törvény az elektronikus hírközlésről
b) 2/2015. (III. 30.) NMHH rendelet az elektronikus hírközlési előfizetői szerződések részletes szabályairól (ESZR)
c) 13/2011 (XII. 27.) NMHH rendelet az elektronikus hírközlési szolgáltatás minőségének az előfizetők és felhasználók védelmével összefüggő követelményeiről, valamit a díjazás hitelességéről
d) 4/2012. (I. 24.) NMHH rendelet a nyilvános elektronikus hírközlés szolgáltatáshoz kapcsolódó adatvédelmi és titoktartási kötelezettségre, az adatkezelés és a titokvédelem különleges feltételeire, a hálózatok és a szolgáltatások biztonságára és integritására, a forgalmi és számlázási adatok kezelésére, valamint az azonosító kijelzésre és hívásátirányításra vonatkozó szabályokról
e) Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet – továbbiakban: **GDPR**),

f) Az információs önrendelkezési jogról és az információbiztonságról szóló 2011. évi CXII. törvény

g) 2013. évi L. Törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

h) 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

5.4. Kommunikáció

Az IBP-t a Cég minden munkatársának ismernie kell, kiemelten azoknak, akik a Cég informatikai rendszerét használják és üzemeltetik. Ez utóbbi esetben az IBP megismerését és tudomásul vételét dokumentálni kell.

6. Alapelvek és célkitűzések

A Cég az informatikai biztonság területén az alábbi alapelveket es védelmi célkitűzéseket kívánja következetesen érvényesíteni a jogszabályi követelményeknek és felügyeleti elvárásoknak megfelelően.

6.1. Célkitűzések

Hitelesség biztosítása a Cég kezelésében lévő adatok tekintetében. Szükséges, hogy minden adat tekintetében minden kétséget kizáróan megállapítható legyen a bekerülő adat forrása és az adat valóságnak történő megfelelősége, valamint annak biztosítása, hogy a bekerülő adatból az informatikai adat előállítása során és azt követően az adat mindvégig megőrizze ezen minőségét.

Bizalmasság biztosítása a kezelt adatok esetében, azaz annak biztosítása, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. Érvényesülését elsősorban az informatikai rendszerben történő adathozzáférések és adatkezelés, valamint a Cég belső és külső kommunikációja során kell biztosítani.

Sértetlenség biztosítása az adatkezelés folyamán, mely biztosítja, hogy az adatok tartalma és tulajdonságai az elvárttal megegyezzenek, ideértve a bizonyosságot abban, hogy azok az elvárt forrásból származzanak (ld. hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

Rendelkezésre állás biztosítása a teljes adatkezelés folyamán, tehát annak biztosítása, hogy az elektronikus információs rendszerek és az azokban tárolt és/vagy kezelt adatok az arra jogosult személyek számára – jogosultsági szintjüknek megfelelően - elérhetőek és felhasználhatók legyenek.

6.2. 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:

a) az összes rendszerelemre
b) a rendszerek architektúrájának minden rétegére, mind a számítástechnikai infrastruktúra, mind az alkalmazások szintjén
c) 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 intézkedés megvalósításra került és azok összességükben szabályozott és szerves egészet alkotnak.

A védelem kockázatarányosságának alapelve – A védelem mértéke és költségei a felmért kockázatokkal arányosak legyenek. Célkitűzés a szükséges és elégséges védelmi költséggel elért maximális védelmi képesség.

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

A védelem folyamatosságának alapelve - Az informatikai rendszerek bevezetése során vagy a fenti alapelvek alapján elérendő megfelelőségi szintek kielégítése érdekében azt követően kialakított védelmi képességeket a rendszer teljes életciklusa alatt folyamatosan biztosítani kell.

6.3. Kritikus sikertényezők

Az Opennetworks számára az információbiztonság sikeres megvalósítása során kritikus tényezők a következők:

- a biztonsági szabályozó környezet pontos meghatározása, megismerése és nyomon követése
- a vezetőség elkötelezettsége
- a biztonsági követelmények, a kockázatelemzés és a kockázatkezelés módszertanának pontos megértése és – a jogszabályi környezetnek megfelelő – helyes és következetes alkalmazása
- hatékony biztonság-menedzsment és ennek érvényesítése valamennyi érintett felé
- gondoskodás a kellő oktatásról és képzésről
- átfogó, mindenre kiterjedő és folyamatos mérési módszer alkalmazása az információbiztonság menedzseléséhez kapcsolódó teljesítőképesség értékeléséhez és a helyesbítési, fejlesztési javaslatok visszacsatolásához.

6.4. Kockázatalapú megközelítés

Az Opennetworks célul tűzte ki – a kockázatokkal arányos védelem biztosítása érdekében – a kockázatelemzés rendszeres, belső szabályozás szerinti elvégzését a fenyegetések, a gyenge pontok, a nem elviselhető kockázatú tényezők meghatározására, valamint az ezek alapján kialakítandó védelmi intézkedési terv és intézkedések meghatározására és megvalósítására.

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

6.5. Szervezeti és felelősségi kérdések

Az IBP-ben lefektetett elvek alsóbb szintű szabályzatokban történő kidolgozásának és betartatásának minden estben kell, hogy legyen felelőse: az Információ Biztonsági Felelős – IBF. Az IBF olyan pozíció, mely – függetlenül attól, hogy a Cég mely más pozíciójában, mely jelentési hierarchia szerint köteles eljárni - e felelősségi körében közvetlenül a Cég vezetőjéhez rendelt pozíció kell, hogy legyen. Az IBP elvek betartásának helyzetéről és a szükséges intézkedésekről az IBF rendszeresen beszámolási kötelezettséggel tartozik a Cég vezetőjének, aki az információ biztonsági feladatok megvalósításának technológiai és személyi feltételeit, valamint a szükséges forrásokat biztosítja. Az IBP betartása minden annak személyi hatálya alá eső (ld. 4.1.) feladata és annak be nem tartása a különböző szabályozásokban és szerződésekben meghatározott szigorú szankciókat vonhat maga után.

7. Célkitűzések az adminisztratív, a fizikai és logikai biztonság területén

7.1. A jogszabályi megfelelőség biztosítása

A Cég a hatályos jogszabályokban történő megfelelőség érdekében a jogi szabályozással érintett rendszer(ek) és az abban kezelt adatok tekintetében:

- Elvégzi az érintett rendszerek biztonsági osztályba sorolását
- ennek alapján elvégzi az adott rendszer biztonsági kockázatelemzését a jogszabályban meghatározott teljesülési kritériumoknak megfelelően
- meghatározza azokat az adminisztratív-, fizikai-, és logikai elvárásokat és célokat, melyeket mindezek alapján az IBP-ben meghatározott alapelvek (B – S – R) és a fentiek alapján teljesíteni kell és intézkedik a végrehajtásukról.

Jelen IBP azon célkitűzéseket tartalmazza, melyeket a szabályozás-kritikus rendszerek esetében teljesíteni szükséges a megfelelő biztonsági szint elérése érdekében, tehát azokat, melyek meghatározzák a Cég szabályozás-kritikus rendszereinek biztonsági osztályához kapcsolódó megfelelőségét.

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

Amennyiben ezen IBP kidolgozását követő biztonsági osztályba sorolás(ok) és a kapcsolódó követelmények esetében bármely olyan tény vagy információ merülne fel, mely a célok módosítását, kiegészítését igényelné, úgy jelen IBP a 8.2. fejezetben meghatározott felülvizsgálat során módosításra kerül.

7.2. Adminisztratív biztonság

Az adminisztratív biztonság területén a Cég vezetésének célkitűzései az alábbiak:

- A Cég folyamatos, zavartalan és hatékony működését, valamint jogszabályi megfelelőségét biztosító informatikai szabályozó környezet és feltételrendszer teljes körű megteremtése és folyamatos gondozása (koncepciók, szabályzatok és eljárásrendek).
- A Cég kialakítja a kockázatelemzés megfelelő eljárásrendjét, valamint ebben és más szabályozó dokumentumokban meghatározottak szerint elvégzi szabályozás-kritikus rendszereinek biztonsági osztályba sorolását.
- Szabályozásaiban meghatározott gyakorisággal és módszertannal végrehajtja a kockázatelemzéseket és a kapott eredményeknek megfelelő intézkedéseket foganatosítja.
- A Cég az informatikai biztonsággal kapcsolatos intézkedési tervet készít, melyben a kockázatelemzésekhez kapcsolódóan feladatokat határoz meg. Ezek teljesítését meghatározott rendszerességgel ellenőrzi, illetve az éves kockázatelemzések kapcsán a terveket aktualizálja.
- Beszerzései során teljesíti a szabályozó környezet által meghatározott elvárásokat a rendszer biztonsági elemeire és egyéb rendszerelemekre, valamint a kapcsolódó dokumentációkra vonatkozóan és szükség esetén azokat szerződéses kötelezettségként a beszerzésekhez kapcsolódó szerződéses megállapodásokban rögzíti.
- A Cég informatikai biztonsági szabályozó környezete kiterjesztésre kerül az érintett rendszerek teljes életciklusára.
- A Cég elektronikus információbiztonsági követelményei szerződéses kötelezettségként kiterjesztésre kerülnek azon szabályozás kritikus külső elektronikus információs rendszerek körére is, melyek

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

szolgáltatásait a Cég információs vagyonának kezeléséhez kapcsolódóan bármilyen módon igénybe veszi.

- A Cég kidolgozza, meghirdeti és végrehajtja a személybiztonsági követelményrendszerét és az erre vonatkozó eljárásrendet.
- A Cég céljának tekinti, hogy az információbiztonság megvalósításához kapcsolódó képzések teljes körűen és minden érintett körében megtörténjenek.

7.3. Fizikai és szervezeti biztonság, környezeti infrastruktúra

A fizikai biztonság területén a Cég vezetésének célkitűzései az alábbiak:

- Az információ kezelésének és feldolgozásának helyet adó objektumok, az egyes eszközök, az abban elhelyezett rendszerek, adattárolók és adathordozók fizikai védelmének biztosítása.
- A szervezeti és objektum biztonság teljes körű megvalósítása.
- Az objektumok, személyek, rendszerek, adatok védelmének biztosítása a különböző incidensek során (pl. elemi kár, tűzeset, áramellátás kimaradása, külső támadások, betörés, illetéktelen hozzáférési kísérletek).
- Adatok értékelése során az előírt fizikai informatikai biztonsági követelmények betartatásának elősegítése.
- Személyi felelősségek egyértelmű meghatározása és elhatározása.

7.4. Logikai biztonság

A logikai biztonság területén a Cég vezetésének célkitűzései az alábbiak:

- Személybiztonság szabályozó rendszerének kialakítása, mely kiterjed a cég teljes személyi állományára, valamint minden olyan személyre, aki a cég szabályozás kritikus elektronikus információs rendszereivel kapcsolatba kerül agy kerülhet.
- A Cég minden szabályozás kritikus elektronikus információs rendszerhez rendszerbiztonsági tervet készít.
- A szabályozás-kritikus rendszerek esetében a konfiguráció kezelés szabályozásának kialakítása és betartása, valamint a rendszer

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

elemeinek és a rendszer alapkonfigurációjának írásos rögzítése és folyamatos karbantartása.

- A szoftverhasználat feltételrendszerének és korlátozásainak meghatározása és betartatása az érintettekkel.
- Az üzletmenet folytonosság feltételrendszerének kidolgozás és a folyamatos üzletmenet biztosítása a rendelkezésre állás alapelvének jegyében.
- A megfelelő működés érdekében a karbantartás szabályozó környezetének kialakítása és az ennek megfelelően végzett rendszeres karbantartások megvalósítása.
- Az adatkezelésre és adatbiztonságra vonatkozó szabályozó környezet kialakítása.
- Az adathordozók védelmére vonatkozó szabályozó környezet kialakítása és az ebben előírt hozzáférési, törlési használati előírások megvalósítása.
- Az azonosításra és hitelesítésre vonatkozó eljárásrend kialakítása és betartása az alkalmazott eszközök és eljárások tekintetében mind a szervezeti, mind a szervezeten kívüli felhasználók esetében.
- Az informatikai rendszerekhez és alkalmazásokhoz való hozzáférési jogok engedélyezésének, valamint a jogosultság ellenőrzés eljárásrendjének kialakítása és annak betartása.
- A rendszer és információ sértetlenség feltételrendszerének kialakítása, a kártékony kódok elleni védelem megvalósítása, a kapcsolódó rendszerfelügyeleti tevékenység megvalósítása, valamint a kapcsolódó esetleges incidensek kezelése.
- Az elszámoltathatóság és számonkérhetőség megvalósítása a naplózási eljárásrend kialakításával és a naplózás ebben foglaltak szerinti megvalósításával.
- A rendszerek határainak védelme.
- Rendkívüli események, incidensek, alaptevékenység kimaradásának elkerülése, kivédése és kezelése a kockázat arányos védelem alapelvének megfelelően.

Opennetworks Kft.
1117 Budapest, Fehérvári út 50-52.
Telefon: +36 1 999-6000 • Fax: +36 1 999-6001
E-mail: info@opennet.hu • Web: www.opennet.hu

8. Záró rendelkezések

8.1. Értelmező rendelkezések

Az IBP-ben használt fogalmak és definíciói a 2013 évi L. törvény fogalmaival és definícióival azonosak.

8.2. Felülvizsgálat

Az IBP-t évente felül kell vizsgálni, a felülvizsgálat az Információ Biztonsági Felelős feladata.