Biztonságpolitika

Besorolás: A (nyilvános)

Verziószám: 10.0

Verzió dátum: 2023.08.16.

Tartalma:

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
7.0	2021-09-07	2021. évi felülvizsgálat – áttekintés, ellenőrzés	Stark Judit, IBF
8.0	2022-07-20	2022. évi felülvizsgálat – kiegészítés és MSZ ISO/IEC 27001:2014 szabvány előírásainak történő megfelelés biztosítása.	Stark Judit, IBF

Aktuális verzió:

9.0	2023-08-16	2023. évi felülvizsgálat – kiegészítés és MSZ ISO/IEC 27001:2014 szabvány előírásainak történő megfelelés biztosítása.	Stark Judit, IBF

A szabályzat

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, valamint, hogy ennek kapcsán Információbiztonság Irányítási Rendszert szükséges kialakítani és fenntartani.
Az információvagyon védelméről átfogó módon gondoskodik a Cég, a rá vonatkozó jogszabályi kötelezettségeket, valamint egyes szabványoknak történő megfelelési szándékot szem előtt tartva.
Az Opennetworks e téren képviselt irányelveit jelen Információ Biztonsági Politikában (a továbbiakban IBP) teszi közzé, ezek megvalósítására Információbiztonság Irányítási Rendszert (IBIR) alakít ki, tart fent és azt folyamatosan tovább fejleszti, melyhez kapcsolódó szabályzatokat és előírásokat Információbiztonsági Dokumentációs Rendszerben (IBDR) rögzíti.
Az IBIR kockázatkezelési folyamat segítségével őrzi meg az információk bizalmasságát, sértetlenségét és rendelkezére állását, célja az érintett felekben bizalmat kelteni a tekintetében, hogy a kockázatokkal a Cégnél kielégítő és szabályozott módon foglalkoznak.
Az Opennetworks vezetése a jelen IBP-ben meghatározott egyetemleges alapelvek és belső biztonsági alapkövetelmények maradéktalan teljesítését várja el valamennyi munkatársától, alvállalkozóitól, beszállítóitól és miden egyéb érdekelt féltől.
A vezetés biztosítja az IBP teljesítéséhez szükséges erőforrásokat, valamint azt, hogy a rá vonatkozó és a betartásához szükséges ismereteteket valamennyi bevont erőforrás elsajátíthassa.
Egyúttal a Cég jelen dokumentumon keresztül garantálja valamennyi külső partnere (ügyfelek, fővállalkozók, munkatársak, alvállalkozók, beszállítók) számára az IBP teljesítését.
Az IBP kivétel nélkül kiterjed az Opennetworks által végzett valamennyi folyamatra, alkalmazott rendszerre és a cég valamennyi szervezeti egységére, részét képezi a szervezet nem biztonsági célú folyamatainak és információs rendszereinek, ezek kialakításánál figyelembe veszik az IBIR folyamatait, betartják az IBIR különböző szintű szabályozásaiban foglalt vonatkozó előírásokat.

3. Az IBP célja

Az IBP az Opennetworks legfelső vezetésének akaratnyilvánítása a cég rendszerei, folyamatai és erőforrásai által kezelt adat-, és információvagyon bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésére és fenntartására irányuló intézkedések kidolgozására, fenntartására és folyamatos fejlesztésére.
Az IBP alapul szolgál továbbá a biztonsági politikánál alacsonyabb szintű folyamatok és szabályozások - így a teljes Információ Biztonság Irányítási Rendszer (IBIR) kialakításához, a jelen és jövőbeli kockázatelemzések lefolytatásához és biztonsági döntések meghozatalához, illetve a biztonsági rendszer működtetői és az érintettek számára a napi rendeltetésszerű tevékenységük gyakorlásához.

Az IBP, a rá épülő biztonsági szabályozás és a kapcsolódó biztonság-irányítási rendszer (IBIR) célja és prioritásai a következők:

- **Megfelelőség: j**ogkövető magatartás és a jó hírnév érdekében védeni a szervezet értékeit. A jogszabályi megfelelőség mellett kiemelt cál az iparági szabványoknak és jó gyakorlatnak, illetve a cég által meghatározott belső szabályoknak, célértékeknek történö
- **Tudatosság, szervezettség:** a hatékonyság és a technikai megoldások használata segítségével növelni az információbiztonságot. Speciális biztonsági intézkedések: például kockázatkezelés, proaktív megelőzés, sebezhetőség-monitorig, védelmi intézkedések együttese szervezett védekezést, hatékonyabb megelőzést biztosít.
- **Elszámoltathatóság: a**melynek középpontjában felelősségi hierarchia áll, formalizált és szabályozott döntéshozatallal és folyamatokkal.
- **I-P-D-R-R (Identify-Protect-Detect-Respond-Recover)**: a kockázat és sérülékenység azonosítás, védelem és megelőzés, a tájékoztatás, az oktatás, a felderítés, értékelés, mérés, visszacsatolás, helyreállítás és a szankcionálás eszközeivel segíteni az intézkedések érvényesítését és a biztonsági szint növelését.

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 és a folyamatokban értintett további munkatársakra)
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 és a folyamatokban értintett további szereplőkre).

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 és kapcsolódó folyamatra, 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
f) folyamatokra.
g) adatokra és adatkezelésre

4.3. Az IBP területi hatálya

Az IBP területi hatálya kiterjed a tárgyi hatálya alá tartozó informatikai 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 és az otthoni munkavégzés folyamataira.

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 – IBDR – 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 közzététele a Cég ügyvezetőjének, karbantartása és folyamatos felülvizsgálata a Cég Informatikai Biztonsági Felelősének (IBF) feladata.
Az IBF az információs és ezen belül kiemelten az informatikai rendszerek és kapcsolódó folyamatok egészére, illetve a rendszerelemek teljes életciklusára vonatkozik, valamint minden kapcsolódó folyamatra, függetlenül attól, hogy érint-e konkrét informatikai rendszert.
Az információs és ezen belül kiemelten az informatikai biztonság elviselhető kockázati szinten tartása érdekében alakítja ki az Opennetworks informatikai biztonsági dokumentációs rendszerét (IBDR), az alábbi elemekkel:

a) Törvényi előírások, egyéb jogszabályok és alkalmazott szabványok 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, a kapcsolódó eljárásrendekkel és dokumentumokkal.

Aktuális IBIR dokumentumok

5.3. Az IBP jogszabályi megfelelősége

A jelen IBP-ben megfogalmazott elvek és intézkedések megfelelnek az érvényes magyar jogszabályoknak, melyek közül az aktuális vonatkozó jogszabályok hivatkozását az IBIR-en belül jelen IBP tartalmazza az alábbiak szerint:

a) 2003. évi C. törvény az elektronikus hírközlésről
b) 20/2020. (XII. 21.) 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 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.
i) Egyúttal az IBP célja az MSZ ISO/IEC 27001:2014 szabvány előírásainak történő megfelelés biztosítása.

5.4. Kommunikáció

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

A Cég az információs 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 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.

Az IBIR dokumentumai és azok minősítése:

Biztonsági elvárás, intézkedés	Aktuális IBDR dokumentum	Dokumentum besorolás
Informatikai Biztonság legfőbb, nyilvános szabályozó dokumentuma: IBP	Biztonságpolitika	Nyilvános -C1
Informatikai biztonsági szabályzat	Információ Biztonsági Szabályzat	Bizalmas - C3
Kockázatelemzési eljárásrend	Kockázatelemzési és kockázatkezelési Szabályzat (IBKESZ)	Bizalmas - C3
Kockázatelemzés és Intézkedési Terv	Core rendszerek kockázatelemzés	Bizalmas - C3
Képzési eljárásrend	Információ Biztonsági Képzési Szabályzat (IBKSZ)	Belső használatra - C2
Biztonsági képzési dokumentumok	Információ biztonság és biztonság tudatosság	Belső használatra - C2
Fizikai védelmi eljárásrend	Fizikai védelmi szabályzat (FVSZ)	Bizalmas - C3
Konfiguráció kezelés, fejlesztés, bug és patch management, rendszer karbantartás	Konfiguráció kezelés, fejlesztés, bug és patch management, rendszer karbantartás	Bizalmas - C3
Üzletmenet folytonosságra és helyreállításra vonatkozó eljárásrend és tervek	BCP/DRP Szabályozás és Terv, BCP/DRP Terv, VPBX	Bizalmas - C3
Incidenskezelési Eljárásrend	Incidenskezelési szabályzat (IKSZ)	Bizalmas - C3
Adathordozók védelmére és szanitálására vonatkozó eljárásrend	Adathordozók Védelme Szabályzat (AVSZ)	Bizalmas - C3
Azonosítási, azonosító-gazdálkodási, hitelesítési, jogosultság-kezelési és ellenőrzési eljárásrend	Hozzáférésbiztonsági Szabályzatok	Bizalmas - C3
Logikai Védelmi Szabályzat	Logikai védelmi szabályzat (LVSZ)	Bizalmas - C3
Naplózási eljárásrend	Naplózási Szabályzat (NSZ)	Bizalmas - C3
Mentési eljárásrend	Mentési Szabályzat (MSZ)	Bizalmas - C3

Adatvédelmi és adatkezelési eljárásrend	Adatvédelmi és Adatkezelési Szabályzat (AASZ)	Belső használatra - C2
Adatkezelési Tájékoztató	https://www.opennet.hu/wp-content/uploads/ON_ASZF_4.sz_melleklet_adatkezelesi_tajekoztato_20220601.pdf	Nyilvános -
Rendszer architektúra rajz	Ld. a Rendszerbiztonsági Terv - ZEUS és ZEUS-kapcsolt szolgáltatások (Telefonáló, Faxoló, VIPeX) (RBT- ZEUS) dokumentumban.	Bizalmas - C3
Adatvagyon leltár, adatgazdák	Adatvagyon leltár	Belső használatra - C2
Rendszerbiztonsági Terv	Rendszerbiztonsági Terv - ZEUS és ZEUS-kapcsolt szolgáltatások (Telefonáló, Faxoló, VIPeX) (RBT-ZEUS)	Bizalmas - C3
Rendszer Üzemeltetési Szabályzat	Rendszer Üzemeltetési Szabályzat - ZEUS és ZEUS-kapcsolt szolgáltatások (Telefonáló, Faxoló, VIPeX) (RÜSZ- ZEUS)	Bizalmas - C3

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) az összes erőforrásra
c) az összes folyamatra
d) a rendszerek architektúrájának minden rétegére, mind a számítástechnikai infrastruktúra, mind az alkalmazások szintjén
e) 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.
A védelem folyamatosságának alapelve – Az információs és 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
• a kockázatok rendszeres elemzése és a kezelésükre vonatkozó célkitűzések és tervek kidolgozása.

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.

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 információs és informatikai rendszerei és az abban kezelt adatok tekintetében:
• elvégzi az érintett rendszerek biztonsági osztályba sorolását
• ennek alapján elvégzi az adott rendszer biztonsági kockázatelemzését
• meghatározza azokat az adminisztratív-, fizikai-, és logikai elvárásokat és célokat, melyeket ezek alapján az IBP-ben meghatározott alapelvek (B – S – R) és a fentiek alapján teljesíteni kell és intézkedik a végrehajtásukról.

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.
• Meghatározza azokat a belső és külső tényezőket, amelyek hatnak arra a képességére, hogy elérje a biztonság irányítási rendszerétől elvárt eredményeket.
• Osztályozza az információs vagyont és az egyes vagyonelemeket besorolásuk szerint kezeli és védi.
• Szabályozásaiban meghatározott gyakorisággal és módszertannal végrehajtja a kockázatelemzéseket ezekre a tényezőkre vonatkozóan és a kapott eredményeknek megfelelő intézkedéseket beépíti az IBIR-be és foganatosítja, majd az intézkedések eredményeit értékeli. A kockázat elemzés alkalmazott módszertana magában foglalja a kockázat elfogadás, illetve kezelés kritériumait.
• Biztosítja, hogy a megismételt rendszeres kockázat elemzések következetes és összehasonlítható eredményeket adjanak.
• A Cég az informatikai biztonsággal kapcsolatos intézkedési tervet készít, melyben a kockázatelemzésekhez kapcsolódóan feladatokat határoz meg és ehhez kockázatgazdákat és határidőket jelöl ki. 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 külső elektronikus információs rendszerek körére is, melyek 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 meghatározza a szükséges felkészültséget azon személy(ek) esetében, akik a felügyeleté alatt olya munkát végeznek, amely hatással van az információbiztonsági teljesítményére.
• A Cég céljának tekinti, hogy az információbiztonság megvalósításához kapcsolódó képzések teljes körűen és minden érintett körében megtörténjenek. Ez az oktatási tevékenység kiterjed az IBP személyi hatálya alá tartozó valamennyi érintett biztonság tudatosságának növelésére is.
• A Cég rendszeresen, tervezett és dokumentált módon értékeli az IBIR teljesítményét.

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.

• Külön intézkedési terv kidolgozása és betartása a Felhőben kezelt és/vagy továbbított adatok és információk biztonságának megőrzésére amennyiben ez az adott folyamat szempontjából releváns.

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 elektronikus információs rendszereivel kapcsolatba kerül agy kerülhet.
• A Cég minden elektronikus információs rendszerhez rendszerbiztonsági tervet készít.
• Az elektronikus információs rendszerekre a konfiguráció kezelés szabályozásának kialakítása és betartása, valamint a rendszer 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, üzletmenet folytonossági és helyreállítási terv kidolgozása és rendszeres tesztelése.
• 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 mentés és naplózás folyamatainak kidolgozása, ennek szabályozása.
• 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 számon kérhetőség 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.

8. Záró rendelkezések

8.1. Értelmező rendelkezések
Az IBP-ben használt fogalmak és definíciói az 5.3 pontban felsorolt jogszabályok és szabvány fogalmaival és definícióival azonosak.

8.2. Felülvizsgálat

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