BUDAPEST FŐVÁROS

III. KER. ÓBUDA-BÉKÁSMEGYER ÖNKORMÁNYZATA

KÖLTSÉGVETÉSI SZERVEKET KISZOLGÁLÓ INTÉZMÉNY

(a továbbiakban: KSZKI)

Budapest, 1033 Folyamőr u. 22.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

TARTALOM

1. BEVEZETÉS

Napjainkban szinte minden folyamat és nyilvántartás informatikai (továbbiakban IT) eszközökön és rendszereken kerül rögzítésre, ezért ezek védelme kiemelt feladat.

2. A 2013. ÉVI L. TÖRVÉNY

az állami és önkormányzati szervek elektronikus információbiztonságáról.

A nemzet érdekében kiemelten fontos - napjaink információs társadalmát érő fenyegetések miatt - a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága. Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

3.1.1.1.1. AZ ÉRINTETT SZERVEZET

A Budapest III. Ker. Óbuda-Békásmegyer Önkormányzata Költségvetési Szerveket Kiszolgáló Intézmény (továbbiakban Szervezet)

3.1.1.1.1.1. ÉRVÉNYESSÉG

Jelen szabályzat kiadásával a korábban érvényben lévő Informatikai Szabályzatok hatályukat veszítik.

3.1.1.1.1.2. FELÜLVIZSGÁLAT

A szabályzatot évente szükséges frissíteni, de abban az esetben, ha az informatikai környezetben jelentős változás történik, haladéktalanul felül kell vizsgálni.

A folyamatos vezetői, IT biztonsági felelősi ellenőrzések mellett a megfelelőségeket belső felülvizsgálatok, ill. külső, független felülvizsgálatok lefolytatásával időszakonként vizsgálni szükséges. A felülvizsgálatoknak az IT biztonságért felelős vezető kezdeményezésre legalább évente (ill. nagyobb változások esetén a változást követően) meg kell történnie.

A vizsgálatok során feltárt eltérésekre a kockázatokkal arányos helyesbítő és megelőző intézkedéseket kell végrehajtani. Az intézkedések kezdeményezése az IT biztonságért felelős vezető tesz javaslatot.

Amennyiben a vizsgálatokhoz szoftvereket, teszt adatbázisokat kell használni, úgy ezeket hozzáférési szempontból elkülönítetten kell kezelni. Az éles rendszereket, meg kell védeni az illegális betekintés, módosítás ellen. A vizsgálatokat úgy kell tervezni, hogy biztosított legyen a kellő mélység, de a vizsgálat a bizalmassági, sértetlenségi, rendelkezésre állási követelményeket ne sértse.

A jogi, törvényi vagy szerződéses kötelezettségek betartása érdekében a következőket kell rögzíteni:

- A releváns jogszabályok követésének szabályai
- A rendelkezésre álló licence-ek
- Adatvédelmi nyilvántartások

A szabályzat eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az informatikai rendszerek biztonságáért felelős személy (továbbiakban: információbiztonsági felelős, rövidítve IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a Szervezet vezetőjének hatásköre.

3.1.1.1.1.3. JOGOSULTSÁGOK

Jelen szabályozás a KSZKI tulajdona, tartalmának megismerésére, csak a Szervezet dolgozói, illetve az informatikai üzemeltetésben részt vevő, külső partnerek jogosultak. A dokumentumot másolni, sokszorosítani, illetve illetéktelen személyekhez juttatni tilos.

3.1.1.1.2 MEGHATÁROZÁSOK

3.1.1.1.2.1.1.CÉLOK

Az Informatikai Biztonsági Szabályzat (továbbiakban IBSZ) elsődleges célja a Szervezet informatikai rendszereinek a jogszabályoknak megfelelő biztonságos és áttekinthető működtetése, illetve a számítástechnikai eszközök beszerzésének informatikai biztonsági szempontból történő szabályozása. A Szervezeten belüli egységes biztonsági szabályozás kialakítása, melynek során a rendszer biztonsági működését hivatottak a bevezetett szabályok biztosítani. Az informatikai biztonsági intézkedésektől csak akkor várható megfelelő eredmény, ha azokat előírásszerűen használják és alkalmazzák.

Az IT Biztonsági Szabályzat további célja, hogy meghatározza az IT biztonsággal kapcsolatos feladatokat és felelősségeket, megteremtse a számon kérhetőség alapjait. A dokumentumnak az alábbi részletes céljai vannak:

- Határozza meg az IT biztonság szervezeti kereteit, az IT biztonsági feladatokat ellátó szerepköröket, azoknak a feladatát, felelősségét és hatáskörét,
- Határozza meg az IT biztonsági intézkedések működtetésével összefüggő feladatokat, amelyeket a mindennapi működés során végre kell hajtani, alkalmazni kell,
- Határozza meg az IT biztonsági intézkedés végrehajtásának felelősét, akin számonkérhető a biztonsági intézkedések működtetése, alkalmazása.
- Határozza meg az IT Biztonsági intézkedés végrehajtásában, alkalmazásában közreműködő egyéb szereplőket, érintettjeit és azok feladatait.

Az Informatikai Biztonsági Szabályzatban meghatározott biztonsági intézkedések részletes végrehajtási utasításait, eljárásait kapcsolódó dokumentumok, mint például üzemeltetési kézikönyvek, felhasználói kézikönyvek tartalmazzák.

Jelen dokumentum a Szervezet magas szintű Informatikai Biztonsági Szabályrendszere (IBSZ), amely támaszkodik az ISO/IEC 27001:2013 nemzetközi szabvány követelményeire, felépítése a szabvány felépítését csak részben követi, illetve megfeleltethetőséget biztosít a 2013. évi L. tv és a kapcsolódó Kormányrendeletek előírásainak.

A szabályzat tartalmazza a Szervezet minden alrendszerére érvényes informatikai biztonsági szabályokat.

3.1.1.1.2.1.3. A SZÁMÍTÁSTECHNIKAI RENDSZEREK ÜZEMELTETÉSÉNEK, FENNTARTÁSÁNAK CÉLJA

A Szervezeten belül található számítástechnikai rendszerek létének kizárólagos célja a munkavégzés biztosítása. Ezért ezen eszközök, a rajtuk zajló folyamatok, a felhasználó által kifejtett aktivitás és a tárolt adatok a munkáltató által bármikor ellenőrizhetőek és rögzíthetőek függetlenül attól, hogy a magáncélú használat engedélyezett-e valamely felhasználó számára vagy sem.

3.1.1.1.2.1.3. A SZABÁLYZATHOZ KAPCSOLÓDÓ DOKUMENTUMOK

- Szervezeti és Működési Szabályzat
- Munkaköri leírások
- Tűzvédelmi Szabályzat
- Beszerzési Szabályzat
- Selejtezési Szabályzat
- Iratkezelési Szabályzat
- Adatvédelmi és adatbiztonsági szabályzat
- Biztonsági Osztályba sorolás
- Kockázatelemzés

Amennyiben a Szervezet úgy ítéli meg, hogy esetében célszerűbb a fenti dokumentumok kialakítása helyett valamely kérdéskört közvetlenül az IBSZ-ben szerepeltetni, úgy ezt megteheti.

JOGSZABÁLYOK

- 1999. évi LXXVI. törvény a szerzői jogról (továbbiakban: Szjt.);
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Infotv.);
- 2012. évi I. törvény a munka törvénykönyvéről
- 2012. évi C. törvény a Büntető Törvénykönyvről.
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: Ibtv.);

- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról;
- 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 (továbbiakban: technológiai végrehajtási rendelet);
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről;
- 2015. évi CXXX. törvény az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról;

SZABVÁNYOK, AJÁNLÁSOK

- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Az információbiztonság-irányítási rendszerek. Követelmények;
- ISO/IEC 27002:2013: Az információbiztonság irányítási gyakorlatának kézikönyve;

3.1.1.1.2.1.2.HATÁLYOSSÁG

A Szabályzat hatálya kiterjed — az érintettek körén keresztül:

SZERVEZETI-SZEMÉLYI HATÁLY

A szabályzat szervezeti hatálya a Szervezet valamennyi olyan szervezeti egységére kiterjed, amely a Szervezet informatikai rendszereit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz.

A szabályzat személyi hatálya kiterjed a Szervezettel munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek a Szervezet informatikai rendszereivel (azt használják, üzemeltetik, fejlesztik, telepítik, javítják stb.), így

- a munkaviszony alapján foglalkoztatott alkalmazottakra;
- a Szervezettel szerződéses kapcsolatban álló természetes és jogi személyekre;
- más szervezetek képviseletében a Szervezet munkahelyein vagy ezek környezetében tartózkodó személyekre;
- a rendszer bármely részén karbantartást végző támogató személyzetre.

TÁRGYI HATÁLY

A szabályzat tárgyi hatálya kiterjed az Szervezet informatikai rendszereire, így az informatikai rendszert alkotó

- környezeti infrastruktúra elemeire;
- hardver eszközökre, készülékekre, berendezésekre;
- szoftverekre;
- adathordozókra;
- dokumentációkra.

A tárgyi hatály kiterjed továbbá az informatikai rendszerekben rögzített, tárolt, feldolgozott vagy továbbított adatokra.

TERÜLETI HATÁLY

A szabályzat területi hatálya kiterjed a Szervezet központi és minden egyéb telephelyére. Továbbá mindazon területekre, ahol a Szervezet informatika használatával a tevékenységét kifejti, függetlenül annak geográfiai elhelyezkedésétől.

A szabályzat területi hatálya nem terjed ki a Szervezet tulajdonában lévő, de bérlőnek tartós használatra átadott fizikai területre abban az esetben, ha a bérlő semmilyen módon nem csatlakozik a Szervezet informatikai infrastruktúrájához.

IDŐBELI HATÁLY

A szabályzat a" Záró rendelkezések" fejezetben meghatározott napon lép hatályba.

3.1.1.1.2.2. SZEREPKÖRÖK

A szabályozott informatikai környezetben az alábbi szerepkörök léteznek:

- Adminisztrátor
- Adatgazda
- Rendszergazda
- Informatikai Biztonsági felelős
- Informatikai Biztonságért felelős felsővezető
- Informatikai Vezető (Informatikai csoportvezető)
- Felhasználó
- Külső tanácsadó
- Külső – erőforrást biztosító szolgáltató
- Külső karbantartó
- Vendég
- Biztonsági auditor

3.1.1.1.2.3. SZEREPKÖRÖKHÖZ RENDELT TEVÉKENYSÉG

A meghatározott szerepkörökhöz az alábbi tevékenységek tartoznak:

- Adminisztrátor
  A rendszer belső karbantartását és felügyeletét végzi.
- Adatgazda
  Fenntartja az adatok sértetlenségét, bizalmasságát.
- Rendszergazda
  Az adott rendszer rendelkezésre állását biztosítja.
- Informatikai Biztonsági felelős
  A biztonsági állapot, és környezet felügyelete, ellenőrzése, javaslattétel.
- Informatikai Biztonságért felelős felsővezető
  Az informatikai biztonság fenntartásának feltételeit biztosítja.
- Informatikai Vezető (Informatikai csoportvezető)
  Koordinálja és irányítja az informatikai szakterületet.
- Felhasználó
  A jogosultságának megfelelő rendszerek, szakszerű használata
- Külső tanácsadó
  Igény szerinti tanácsadói tevékenység
- Külső – erőforrást biztosító szolgáltató
  Az üzemeltetéshez szükséges erőforrások biztosítása, ezek karbantartása, javítása.
- Külső karbantartó
  Kiszervezett tevékenységek elvégzése.
- Vendég
  Céljának és engedélyeinek megfelelő tevékenységek végzése.
- Biztonsági auditor

A biztonsági állapot felülvizsgálata, tanúsítása.

Folyamatosan követni kell az IT biztonság tekintetében releváns jogszabályokat és a Szervezet által kötött szerződések IT biztonságot érintő összetevőit. Az informatikai biztonságot meghatározó belső szabályozást a releváns jogszabályok változása esetén aktualizálni szükséges.

Az informatikai biztonságot érintő jogszabályok változásának követése az IT biztonságért felelős vezető feladata. A jogszabályok megváltozása esetén az IT biztonságért felelős vezető feladata, hogy szükség esetén javaslatot tegyen intézkedésekre, folyamatok, eljárások módosítására. Amennyiben szerződés keretében keletkezik új, informatikai biztonságra vonatkozó követelmény, a projektvezető feladata a követelmény jelzése az IT biztonságért felelős vezetőnek.

A szoftverek jogtisztaságának betartása érdekében a szoftverek használatához szükséges licenszekről nyilvántartást kell vezetni. A licence nyilvántartás kérdése hozzákapcsolódik más IT eszközök nyilvántartásához. A licenszek nyilvántartása az IT üzemeltetés, a nyilvántartás értékelése az IT biztonságért felelős vezető feladata. Amennyiben licensz-igény következik be, az IT biztonságért felelős vezető tesz javaslatot a probléma feloldására.

Az Információs önrendelkezési jogról és az információszabadságról szóló törvénynek való megfelelés érdekében el kell készíteni és folyamatosan naprakészen kell tartani a törvény által előírt adatvédelmi nyilvántartásokat. A nyilvántartások elkészítése és karbantartása az adatvédelmi felelős felelőssége. A nyilvántartás elkészítéséhez az Adatgazdáknak információt kell nyújtaniuk.

3.1.1.1.2.3. SZEREPKÖRÖKHÖZ RENDELT FELELŐSSÉG

A meghatározott szerepkörökhöz az alábbi felelősségek kapcsolódnak:

- Adminisztrátor
  Felelős a rendszer sértetlenségéért.
- Adatgazda
  Felelős a rendszer bizalmasságáért.
- Rendszergazda
  Felelős a rendszer rendelkezésre állásáért.
- Informatikai Biztonsági felelős
  A biztonsági állapot, környezet fenntartásáért és fejlesztéséért felel.
- Informatikai Biztonságért felelős felsővezető
  Felel a szükséges erőforrások biztosításáért, a szabályok betartásáért.
- Informatikai Vezető (Informatikai csoportvezető)
  Felelős a terület szakszerű, és jogszerű működéséért.
- Felhasználó
  Felel az általa használt rendszerekben rögzített adatok hitelességéért, és a szabályok betartásáért.
- Külső tanácsadó
  A szakszerű és jogszerű tanácsadói tevékenységéért.
- Külső – erőforrást biztosító szolgáltató
  Az üzemeltetéshez szükséges erőforrások rendelkezésre állásáért felel.
- Külső karbantartó
  A Kiszervezett tevékenységek elvégzéséért.
- Vendég
  Az engedélyezett tevékenysége körében rögzített, átadott adatokért, és a szabályok betartásáért felel.
- Biztonsági auditor

Jogszabályban vagy szabványban rögzített állapot tanúsításáért, a tevékenysége során feltárt hiányosságok közléséért felel.

3.1.1.1.2.4. ÁLTALÁNOS SZABÁLYOK

A felhasználó jogosult e szabályzat megismerésére, a munkavégzéséhez szükséges informatikai infrastruktúrához való hozzáférésre.

A felhasználó nem jogosult a magáncélú felhasználás során keletkezett anyagainak elkülönítésére és tárolására a munkaállomásokon.

A felhasználó köteles e dokumentumban leírt szabályokat betartani. E dokumentumtól egyéni megegyezés keretében el lehet térni. Az eltérést jóvá kell hagynia az IT csoportnak, vagy az Intézményvezetőnek.

Az informatikai rendszer elemeit a felhasználónak rendeltetésszerűen kell használnia hardverek, szoftverek és szolgáltatások tekintetében egyaránt. A felhasználó az eszközöket csak a felelős vezető vagy e szabályzat kifejezett engedélyével használhatja munkáján kívüli célra.

A felhasználó köteles együttműködni a rendszerüzemeltetésért felelős személyekkel (üzemeltetők) olyan esetekben, amikor a felhasználó tevékenysége az informatikai rendszerrel kapcsolatos feladatokat generál.

A felhasználói jelszó felhasználásával történt valamennyi tevékenységért az adott felhasználó kizárólagosan felel.

A felhasználó nem jogosult önállóan, az üzemeltetővel való egyeztetés nélkül szoftvert telepíteni a gépére.

A felhasználó nem jogosult önállóan, az üzemeltetővel való egyeztetés nélkül szoftvert törölni a gépéről, még akkor sem, ha átvételkor nem szerepelt a hivatkozott szoftver a nyilvántartásban.

A felhasználó nem jogosult önállóan, az üzemeltetővel való egyeztetés nélkül az általa használt szoftver, vagy modul módosítására, frissítésére, sem ezek automatizált végrehajtásának engedélyezésére, tiltására.

SZOFTVEREK TELEPÍTÉSE – MÓDOSÍTÁSA – TÖRLÉSE

A felhasználó nem jogosult a Szervezet szoftvereit magáncélra lemásolni, sem más gépre telepíteni.

A felhasználó a Szervezet szoftverhasználatra vonatkozó politikáját követi.

Az Informatikai biztonsági felelős legalább évente áttekinti a szoftverhasználati tevékenységeket, és erről jelentést készít az informatikai vezetőnek.

HARDVEREK KEZELÉSE

A számítógépeket szétszedni, konfigurációjukat, beállításaikat és a rajtuk lévő jelzéseket (pl. nyilvántartási szám, gyári szám stb.) megváltoztatni szigorúan tilos! Amennyiben e jelölések sérülését, eltűnését észleli a felhasználó, köteles azt haladéktalanul bejelenteni az üzemeltetőnek.

Az asztali és hordozható számítógépek konfigurációját és jelzéseit kizárólag az üzemeltető szakemberei változtathatják meg, még abban az esetben is, ha ez időszaki működésképtelenséget okoz.

Az asztali számítógépek és más informatikai berendezések fizikai helyének, gyengeáramú informatikai kábelezésének megváltoztatására kizárólag az üzemeltető szakemberei jogosultak. A kábelezés megváltoztatásának minősül a külső perifériák kábeleinek csatlakoztatása/módosítása.

Az asztali számítógépek villamos kábelezésének megváltoztatására kizárólag az üzemeltető szakemberei jogosultak.

A felhasználó köteles a használatra kapott eszközök külső felületének tisztán tartásáról gondoskodni. A tisztításhoz szükséges kellékanyagokat és igény esetén a betanítást az üzemeltető biztosítja.

Tartózkodni kell minden olyan tevékenység végzésétől a berendezések közelében, ami az üzemszerű működést akadályozni képes, illetve hiba, vagy elektromos zárlat okozására alkalmas.

MOBIL ÉS HORDOZHATÓ ESZKÖZÖK HASZNÁLATA, CSATLAKOZTATÁSA

A mobil eszközök abból adódóan, hogy használatba kerülnek a belső védett környezeten kívül is, különös körültekintést igényelnek. A felhasználó felelős a mobil eszköz fizikai védelméért, lopás elleni védelméért, és a megfelelő környezetben való használatáért.

A mobil eszközt tilos autóban hagyni, nyilvános helyen lopás lehetőségének kitenni: például, de nem kizárólag asztal mellé letett táskában tárolni, bármilyen külső zsebben tárolni, lezáratlan belső zsebben tárolni.

A mobil eszközt tilos úgy idegen hálózaton használni, hogy a felhasználó nem bizonyosodott meg az informatika által előírt adatvédelmi eszközök helyes működéséről a mobil eszközön.

A mobil eszközökön a hálózat helyére, illetve elérési adataira utaló feljegyzést, biztonsági mentést tárolni tilos.

A mobil eszközök elektromos, illetve adathálózatra történő időszaki, vagy állandó csatlakoztatása engedélyhez kötött.

E-MAIL HASZNÁLATA

A Szervezet a saját levelezőrendszerét használja.

A Szervezet alkalmazottai amennyiben munkájuk indokolja, hozzáférést kaphatnak az elektronikus levelezési rendszerhez.

A központi, Szervezeti levelezőrendszer kizárólagos célja a munkavégzés. A felhasználó nem jogosult magáncélra használni a levelezőrendszert.

Az Szervezet által kiosztott minden e-mail cím a munkavégzést, ügyek intézését szolgálja függetlenül attól, hogy egy-egy felhasználó személyéhez kötött az elnevezés. A levelezésbe a munkáltató betekinthet. A Szervezet jogosult az e-mail címmel és az ottani adatokkal minden egyéb műveletre is, például, de nem kizárólag: átirányítani, megszüntetni, automatikus válaszüzenetet applikálni, biztonsági mentést készíteni a levelekről, azokat tárolni, letörölni, publikálni, megosztani más felhasználókkal a céges munkavégzés céljából.

A munkaállomásokon szigorúan tilos a magánlevelezés mellékleteinek, csatolmányainak megnyitása, illetve ezek tárolása.

A fogadott levelekben szigorúan tilos megnyitni, a nem ellenőrzött tartalmú mellékleteket, ismeretlen linkeket.

AZ ELEKTRONIKUS LEVELEZÉS BIZTONSÁGI ELŐÍRÁSAI

Az elektronikus levelezés a Szervezet informatikai rendszereinek biztonságára nézve az egyik fő veszélyforrás, ezért az elektronikus levelezés biztonsága érdekében az alábbi előírásokat kell betartani:

- A számítógépre telepített, naprakész (legalább naponta frissülő) vírusadatbázissal rendelkező vírusvédelmi szoftver nélkül tilos az elektronikus levelezés használata. Jelenteni kell a Helpdesk-en, ha valamilyen oknál fogva a számítógépen nem fut vírusvédelmi szoftver, vagy nem frissül a vírusdefiníciós adatbázisa és a szoftver azt jelzi, hogy az adatbázis elavult.
- Tilos megnyitni a vírusvédelmi szoftver által fertőzöttnek jelzett leveleket, ezeket megnyitás nélkül törölni kell.
- Az elektronikus levélben küldött vírusok általában csatolt fájlként érkeznek. Mivel a vírusvédelmi szoftverek nem ismernek fel azonnal minden új vírust vagy vírusváltozatot, a számítógép akkor is megfertőződhet, ha

naprakész a vírusvédelmi szoftver vírusadatbázisa, ezért a csatolt fájlok megnyitásakor mindig óvatosan kell eljárni.

- A fokozott vírusveszély miatt tilos a nem megbízható forrásból származó levelet, azok levélmellékletét megnyitni, a levélben található internetes hivatkozásokra (linkekre) kattintani. A forrást nem megbízhatónak kell tekinteni, ha
    - a levél feladója nem ismert (az is előfordulhat, hogy ismerőstől érkezik egy vírusos levél, akinek a számítógépe megfertőződött és tudtán kívül terjeszti a vírust);
    - a levél nyelve nem várt, nem külföldi partnerrel folytat a felhasználó levelezést (a sok veszélyes levél idegen nyelvű, ezért ezeket a leveleket fokozott figyelemmel kell vizsgálni);
    - a levél címzettje közt sok, nem ismert személy szerepel;
    - a levél tárgya nem illeszkedik a Szervezet ügyviteli folyamataihoz;
    - levélszemétre jellemző csalogató szövegeket tartalmaz nyereményről vagy pikáns képekről, vagy valamely megvásárolható terméket vagy szolgáltatást reklámoz stb.;
    - a felhasználó számára ismeretlen kiterjesztésű vagy tiltott csatolt fájlokat tartalmaz.

A „Levélszemét” mappába érkező leveleket a kéretlen leveleket szűrő szoftver minősítette levélszemétnek. A szoftver nem minden esetben dolgozik helyesen, lehetnek az ügyviteli folyamathoz tartozó levelek is a mappában. Az itt található levelek megbízhatóságát fokozott figyelemmel kell vizsgálni.

Tilos válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy a Szervezet biztonsági rendszeréről vagy a felhasználó saját hozzáférési adatairól (felhasználónév, jelszó) adjon tájékoztatást.

A levelező szervert is el kell látni olyan hatékony vírusvédelmi szoftverrel, amely megakadályozza a fertőzések elektronikus levelekben történő terjedését.

TILTÓ RENDELKEZÉSEK AZ ELEKTRONIKUS LEVELEZÉSRE VONATKOZÓAN

Az elektronikus levelezés használata során nem engedélyezettek az alábbi tevékenységek:

Szigorúan tilos a levelezési rendszeren keresztül olyan tartalmú levelet küldeni, amely más természetes vagy jogi személy személyiségi, illetve egyéb jogait sérti (pl.: rágalmazás, szerzői jogok megsértése).

Szigorúan tilos a Szervezet jó hírnevét veszélyeztető, a közízlést sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét bántó tartalmú levelek küldése.

Tilos a levelező rendszeren keresztül belső használatú, bizalmas vagy titkos dokumentumokat, adatokat a Szervezetből engedély nélkül kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni.

Tilos a beérkező leveleket a Szervezeten kívüli postafiókba irányítani.

Tilos a levelező rendszerben lánclevelet, azaz olyan levelet továbbítani, amely arra szólít fel, hogy minél több címzettnek küldjünk tovább.

Tilos feliratkozni nem szakmai jellegű, nem az ügyviteli munkát segítő hírlevél küldő szolgáltatásra.

Tilos engedély nélkül a Szervezet teljes címtára felhasználásával szervezeti szintű körlevelet küldeni. Szervezeti szintű körlevelet csak az erre kijelölt (és megfelelő jogosultságot kapott) személyek küldhetnek, ilyen igény esetén a küldendő levélmintát nekik kell eljuttatni.

Tilos másvalaki nevében levelet küldeni, kivéve felelős vezetői utasítás alapján.

KORLÁTOZÁSOK AZ ELEKTRONIKUS LEVELEZÉS HASZNÁLATÁBAN

Az elektronikus levelezés biztonsága és a levelező szerver védelme érdekében az alábbi levelezésre vonatkozó korlátozások vannak érvényben:

- A postafiókok mérete fő szabály szerint 2 Gb. Szükség esetén ettől eltérő kapacitást az informatikai vezető külön kérésre engedélyezhet.
- A beérkező levelek maximális megengedett mérete általában 15 Mb.
- A küldött levelek maximális megengedett mérete általában 15 Mb. Szükség esetén ettől eltérő kapacitást az informatikai vezető külön kérésre engedélyezhet.
- A levelezésben nem fogadhatók és küldhetők levélmellékletként (még tömörített csomagban sem) az alábbi formátumú fájlok a vírusfertőzés veszélye miatt:
    - futtatható fájlok (.exe, .com, .bat, .cmd, .vbs);
    - egyéb programkódot tartalmazó veszélyes fájlok (.dll, .sys, .inf, .bin, .hta, .docm, .xlsm).

A felhasználók feladata gondoskodni a feleslegessé vált leveleik törléséről, a szerveren biztosított tárhely elfogyásakor a levelek archiválásáról. Az archiválás végrehajtásához a Helpdesk-en bejelentve segítség kérhető az Üzemeltetéstől.

AZ ELEKTRONIKUS LEVELEZÉS MAGÁNCÉLÚ HASZNÁLATA

Mivel minden levelezést a Szervezet tulajdonát képező vagy általa bérelt informatikai erőforrások biztosítanak, ezért a levelek is a Szervezet tulajdonát képezik. Így a Szervezet fenntart minden jogot a levelek kezelésével kapcsolatban.

A fentieken túl kerülni kell az Interneten elérhető ingyenes levelezési oldalak vagy magán előfizetésekhez tartozó postafiókok belülről történő használatát. Ezeket hivatalos ügyekben használni tilos.

AZ ELEKTRONIKUS LEVELEZÉS ELLENŐRZÉSE

A Szervezet fenntartja a jogot a levelezés forgalmának naplózására, a levelezés méretének, gyakoriságának, és ha szükséges tartalmának ellenőrzésére, korlátozására a levelező szerver és az Internet kapcsolat sávszélességének hatékonyabb kihasználása, valamint a Szervezet informatikai rendszereinek biztonsága érdekében.

A fenti ellenőrzéseket az Üzemeltetés felsővezetői, vagy az IBF kérésére esetén végzi.

3.1.1.1.2.5. BELSŐ EGYÜTTMŰKÖDÉS

A fentiekben felsorolt szerepkörökben munkát végző személyeknek, illetve vállalkozásoknak, a biztonsági állapot fenntartása, illetve fejlesztése érdekében szoros együttműködésben kell eljárniuk. Minden a feladataik végrehajtását érintő körülményt kötelesek dokumentálni, illetve közölni egymással.

3.1.1.1.3. AZ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT RENDSZERBIZTONSÁGGAL KAPCSOLATOS TERÜLETI SZABÁLYOZÁSAI

3.1.1.1.3.1. KOCKÁZATELEMZÉS

Az információbiztonsági kockázatelemzés célja, hogy

a) vizsgálja az informatikai rendszerek gyenge pontjait (sérülékenység vizsgálat);

b) feltárja az informatikai rendszerekre ható fenyegető tényezőket, veszélyforrásokat (fenyegetettség elemzés);

c) elemezze a veszélyforrások által a gyenge pontokon keresztül bekövetkező sikeres támadások bekövetkezési valószínűségét és az általuk okozott kár nagyságát (kockázatelemzés);

d) valamint kezelje a Szervezet által el nem fogadható kockázatokat (kockázatkezelés). A kockázatelemzés végrehajtása során a következő Kockázatelemzési és kockázatkezelési eljárásrendet kell alkalmazni:

KOCKÁZATELEMZÉSEK FOLYAMATA

Az IBF-nek évente el kell végeznie az informatikai rendszerek kockázatelemzését a jelen eljárásrendben foglalt módszertannak megfelelően.

A kockázatelemzés eredményét a *Kockázatelemzési jelentésben* kell dokumentálni, amelyet jóváhagyás és az érintettek számára kihirdetés céljából be kell terjeszteni az informatikai vezető és a Szervezet vezetője részére.

Jóváhagyás után az informatikai vezető irányításával és a rendszergazda közreműködésével a nem tolerálható kockázatokra *Kockázatkezelési tervet* kell készíteni, amelyet a Szervezet vezetőjének jóváhagyása után, ütemezett és dokumentált módon végre kell hajtani.

A kockázatkezelő intézkedések végrehajtása után az IBF-nek maradványkockázat elemzést szükséges végrehajtani, melynek célja, hogy kimutassa a kockázatkezelő intézkedések eredményességét és feltárja az esetlegesen megmaradó kockázatokat.

A kockázatelemzést ismételten el kell végezni, ha változás következik be az informatikai rendszerekben vagy azok környezetében (beleértve az új fenyegetések és sérülékenységek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az informatikai rendszerek biztonsági állapotát.

A kockázatelemzést legalább évente felül kell vizsgálni, újra el kell végezni figyelembe véve a változásokat.

A kockázatelemzés és a hozzá kapcsolódó dokumentumok bizalmas minősítésűek. Gondoskodni kell a dokumentumok megfelelő védelméről. A kockázatelemzési dokumentumokat kizárólag az érintettek kezelhetik, illetékteleneknek nem adhatják tovább.

KOCKÁZATELEMZÉSI MÓDSZERTAN

A Szervezetnél alkalmazott kockázatelemzési módszertan röviden a következő:

Kezdeti helyzetfelmérés

Az informatikai rendszer kockázatelemzésének elvégzéséhez fel kell mérni, meg kell ismerni az informatikai rendszert és a jelenlegi információbiztonsági állapotát.

A következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:

a) Adminisztratív védelmi intézkedések:
    a. a Szervezetre vonatkozó jogszabályok, szabályzatok;
    b. az informatikai rendszerre vonatkozó szabályzatok;
    c. üzemeltetési eljárások;
    d. szerződések, külső partnerek kezelése;
    e. biztonsági események kezelése.

b) Fizikai védelmi intézkedések:
    a. beléptetés;
    b. az épületben történő közlekedés;

c. a szerverterem kialakítása;

d. az irodák kialakítása;

e. a tiszta asztal, üres képernyő politika alkalmazása.

c) Logikai védelmi intézkedések:

a. szoftverfejlesztés, változáskezelés;

b. a szervizelés, eszközcsere, selejtezés folyamata;

c. mentési megoldások;

d. a jogosultsági rendszer, a jogosultságigénylés folyamata;

e. vírusok és egyéb kártevők elleni védekezés;

f. biztonsági frissítések telepítése;

g. naplózás, biztonsági rendszerek;

h. a hálózat felépítése;

i. kriptográfiai (titkosítási) megoldások.

VAGYONELEMEK MEGHATÁROZÁSA

Az informatikai rendszerre ható fenyegető tényezők különbözőek, attól függően, hogy a rendszer melyik összetevőjét (vagyonelemét) fenyegetik, mert az egyes vagyonelem csoportoknak eltérőek a gyenge pontjaik.

A gyenge pontok és a fenyegető tényezők megfelelő azonosítása érdekében a következő vagyonelem csoportokat kell a kockázatelemzésben vizsgálni:

a) környezeti infrastruktúra;

b) hardverek;

c) szoftverek;

d) adatok;

e) adathordozók;

f) kommunikáció;

g) dokumentációk;

h) humán erőforrások.

Gyenge pontok meghatározása

A helyzetfelmérés alapján megszerzett információk birtokában meg kell határozni az egyes vagyonelemek gyenge pontjait.

Az egyes vagyonelemek gyenge pontjait és a fenyegető tényezőket a KIB 25. számú ajánlása (25/1-3. kötet: Az Információbiztonság Irányításának Vizsgálata 1.0 verzió „gyenge pontok” és „fenyegetettségek” segédletei) alapján érdemes azonosítani.

FENYEGETŐ TÉNYEZŐK ELEMZÉSE

Az egyes vagyonelemekre ható fenyegetések, fenyegető tényezők (pl.: üzleti hírszerzés, rosszindulatú hackerek, természeti katasztrófák) mindig a gyenge pontokon keresztül fejtik ki hatásukat.

Meg kell vizsgálni, hogy a beazonosított gyenge pontokon keresztül mely fenyegető tényezők tudják kifejteni a káros hatásukat.

KÁRÉRTÉK SZINTEK MEGHATÁROZÁSA

A bekövetkezett káresemény súlyosságának, mértékének jellemzésére a következő kárérték szintek kerültek kialakításra:

a) 1 – Kicsi;

b) 2 – Közepes;

c) 3 – Nagy.

A kárérték szintek meghatározása során azt kell figyelembe venni, hogy

a) milyen tényleges vagy erkölcsi kárt jelentene a rendszerben tárolt adatok bizalmasságának sérülése;

b) milyen következményekkel járna a rendszer ideiglenes elérhetetlensége vagy az adatok sérülése, elvesztése;

c) mennyibe kerülne a meghibásodott eszközök javítása, cseréje;

d) mennyi munkaidő ráfordítással járna a helyreállítás.

A kockázatok megállapításához az informatikai rendszer vagyonelemeire rá kell vetíteni a kárérték szinteket.

BEKÖVETKEZÉSI VALÓSZÍNŰSÉGEK MEGHATÁROZÁSA

A következő lépésként meg kell becsülni a fenyegetések bekövetkezési valószínűségét.

A bekövetkezési valószínűséghez a következő értékeket kell használni:

a) 1 – Kicsi (pl. évente vagy több évente következhet be);

b) 2 – Közepes (pl. havonta bekövetkezhet);

c) 3 – Nagy (pl. hetente, naponta bekövetkezhet).

KOCKÁZATOK MEGHATÁROZÁSA

Az információbiztonsági kockázatokat a fenyegetés bekövetkezésének a valószínűsége és az okozott kárt jellemző kárérték szint szorzata fogja megadni.

A kockázatok nagyságának, értékének meghatározásához a következő kockázati mátrixot kell használni:

Kárérték	**Bekövetkezés valószínűsége**		
	1	2	3
1	1	1	2
2	1	2	3
3	2	3	3

A táblázatban a kockázatok jelentése a következő:

a) 1 – Alacsony;

b) 2 – Közepes;

c) 3 – Magas.

NEM TOLERÁLHATÓ KOCKÁZATOK MEGHATÁROZÁSA

A Szervezet azt a döntést hozta, hogy minden közepes és magas kockázatot kezelni kíván.

Ennek megfelelően a toleranciamátrix a következő:

Kárérték	**Bekövetkezés valószínűsége**		
	1	2	3
1	T	T	NTH
2	T	NTH	NT
3	NTH	NT	NT

A táblázatban alkalmazott jelölések értelmezése a következő:

a) T – Tolerálható;

b) NTH – Nem tolerálható, hosszú távon kockázatkezelést igényel;

c) NT – Nem tolerálható, azonnali kockázatkezelést igényel.

KOCKÁZATOK KEZELÉSE

A Szervezet a kockázatokat a következőképpen kezeli:

a) Megfelelő intézkedésekkel csökkenti a fenyegetés bekövetkezési gyakoriságát vagy hatását (kockázat csökkentés).

b) Elkerüli a kockázatot azáltal, hogy az érintett tevékenységet felfüggeszti (kockázat elkerülés).

c) Áthárítja a kockázatot pl. biztosítással vagy megfelelő beszállítói szerződésekkel (kockázat áthárítás).

d) Tudatosan, a következményeket felmérve elfogadja a kockázatot (kockázat elfogadás).

KOCKÁZATCSÖKKENTŐ INTÉZKEDÉSEK

A kockázatcsökkentő intézkedések az alábbi módon csoportosíthatók:

a) Megelőző jellegű intézkedések (preventív kontrollok)
A hibák, sérülékenységek, gyenge pontok, illetve ezek kihasználására való lehetőségek kiküszöbölése.

b) Korlátozó vagy javító intézkedések (korrektív kontrollok)
A veszélyek hatását csökkentő, enyhítő óvintézkedések, további tevékenységek szükségessége nélkül.

c) Észlelő és reagáló intézkedések (detektív kontrollok)
A sérülékenységek, gyenge pontok támadásának észlelése, ártalmas kihatások enyhítésére, illetve válaszreakciók kidolgozása.

KOCKÁZATELEMZÉSEK DOKUMENTÁLÁSA

A Szervezet a kockázatelemzés eredményét a Kockázatelemzési jelentésben, a kockázatkezelő intézkedéseket a *Kockázatkezelési tervben* dokumentálja.

KOCKÁZATELEMZÉSI JELENTÉS

A *Kockázatelemzés jelentés* két részből tevődik össze:

a) egy táblázatos részből, amely a módszertannak megfelelően rögzíti az elvégzett a kockázatelemzés adatait;

A táblázatos résznek tartalmaznia kell:

a) az informatikai rendszer feltárt gyenge pontjait;

b) a gyenge pontokra ható fenyegető tényezőket;

c) a fenyegető tényezők bekövetkezési valószínűségét;

d) a fenyegetés bekövetkezése esetén a kár mértékét jellemző kárértéket;

e) a valószínűség és a kárérték alapján megállapított kockázat mértékét;

f) vázlatosan a javasolt kockázatkezelő intézkedéseket;

g) a javasolt éves ütemezést a kockázatkezelő intézkedések megvalósítására.

A szöveges részben – hivatkozva a táblázatos rész kapcsolódó sorára – részletesen ki kell fejteni:

a) a felmérési állapotot: az azonosított konkrét fenyegetés, veszélyforrás részleteit;

b) a fenyegetés által jelentett kockázatot: a fenyegetés bekövetkezésének módját, a bekövetkezett káresemény és a következmények részleteit, ha a kárérték szintje nagy, a kár elhárításának becsült költségét és/vagy munkaidő ráfordítását;

c) a megállapított kockázat mértékét (alacsony, közepes, magas);

d) a kockázatkezelő intézkedésre tett javaslatot.

KOCKÁZATKEZELÉSI TERV

A Szervezet a nem tolerálható kockázatok kezelésére *Kockázatkezelési tervet* készít.

A tervben a *Kockázatelemzési jelentés* szöveges részéből kiindulva meg kell határozni a megvalósítandó kockázatkezelő intézkedéseket, a szükséges munkaidő ráfordítást és esetleges költségeket, valamint a felelősöket és a határidőket.

3.1.1.1.3.2. BIZTONSÁGI HELYZET-, ÉS ESEMÉNYÉRTÉKELÉS ELJÁRÁSI RENDJE

Az eljárásrend célja az informatikai rendszer használata során bekövetkezett nem kívánatos eseményeket követő vizsgálati folyamat bemutatása.

A vizsgálat egyedi események vagy azonos események elemzésére képes, és ezek hátterében álló okok feltérképezésére.

A feltárási folyamat lépései:

ADATGYŰJTÉS

Minden az esemény kapcsán közvetve, vagy közvetlenül keletkezett releváns adatot, pontos megjelölésével kell összegyűjteni.

CÉLMEGHATÁROZÁS

A vizsgálat célja az esemény bekövetkezését kiváltó okok, továbbá a bekövetkezéshez hozzájáruló tényezők teljes feltárása. A feltárás után meg kell határozni azokat az intézkedéseket, eljárásokat, ami potenciálisan csökkenteni képes az ismétlődés kockázatát.

VÁRHATÓ EREDMÉNY

A vizsgálat után alapvetően három kérdésre kell választ kapni:

- Mi történt?
- Miért történt?
- Hogyan tudjuk megakadályozni?

A VIZSGÁLAT SZÜKSÉGESSÉGE

A vizsgálatot minden olyan esetben le kell folytani, ha olyan esemény következik be, ami a kockázatelemzési táblázatban meghatározott módon nagy valószínűséggel következett be, illetve a hozzá kapcsolódó kárérték magas. (Nem felvállalható kockázat)

3.1.1.1.3.3. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER ÉS INFORMÁCIÓTECHNOLÓGIAI SZOLGÁLTATÁS BESZERZÉS

Bármely informatikához kapcsolódó szolgáltatást nyújtó szolgáltató, ill. alvállalkozó, valamint más együttműködő partnerrel való együttműködés megkezdése előtt a szerződést előkészítő munkatárs az informatikai biztonságért felelős vezető bevonásával megvizsgálja a felmerülő informatikai biztonsági kockázatokat, hozzáférési igényeket, és a szükséges kontrollokat beépíti a partnerrel kötött szerződésbe, kapcsolódó megállapodásba. Szolgáltató, ill. alvállalkozó bevonása miatt fellépő új kockázat felmerülésekor a kockázatot az informatikai biztonságért felelős vezető a kockázat-felmérési eljárások során kezeli.

A külső partnerek képviselőivel a mindenkor hatályos IBSZ vonatkozó részeit a feladatnak megfelelő mértékben ismertetni kell. A betekintés mélységének meghatározása az IT felelős munkatárs (adatgazda) felelőssége. A szerződéskötés és az együttműködés során biztosítani kell, hogy a külső partner (fejlesztő cég) az általa telepített, fejlesztett informatikai rendszert úgy konfigurálja, hogy annak minden eleme és egésze eleget tegyen az IBSZ-ben előírtaknak.

A már meglévő rendszerek cseréje, megújítása esetén meg kell vizsgálni, és szükség esetén az aktuális kockázatoknak megfelelően módosítani kell a belső besorolást. Új rendszerek bevezetésénél el kell végezni a rendszerek besorolását.

3.1.1.1.3.4. BIZTONSÁGGAL KAPCSOLATOS TERVEZÉS

Az informatikai környezet bármilyen változtatásánál (fejlesztés, javítás, csere), meg kell vizsgálni, hogy a rendszerrel szemben támasztott biztonsági követelmények, a változtatás elvégzése után is fennálnak-e, esetleg azokat meghaladja, a kialakított biztonsági szint.

3.1.1.1.3.5. FIZIKAI ÉS KÖRNYEZETI VÉDELEM SZABÁLYAI, JELLEMZŐI

Az illetéktelen fizikai behatolás, károkozás, rongálás, a vagyontárgyak fizikai károsítása, eltulajdonítása és egyéb fizikai jellegű negatív események megelőzése, ill. hatásuk mértékének csökkentése érdekében a Fizikai Biztonsági Szabályzatban foglaltakat kell alkalmazni. Ennek megfelelően rögzíteni kell a következő szabályokat:

- Az épületek és helyiségek védelmére vonatkozó szabályok
- A berendezések védelmére vonatkozó szabályok
- Biztonsági szabályzat-vagyon és objektumvédelem (őrzés, távfelügyelet, átjelzés)
- Fizikai védelmi rendszerek
- Elektronikus jelző és videó-rögzítő rendszerek
- Nyitás- zárás rendszere (kulcskezelés)
- Tiszta asztal - üres monitor process alkalmazása (hozzáférésre utaló jelzések nélkül)

JELSZÓHASZNÁLAT, -BIZTONSÁG

A munkaállomások és hálózati erőforrások használatához jelszó használata kötelező.

A jelszavak minimális hossza 8 karakter, tartalmaznia kell min. 1 kis betűt, 1 nagybetűt és 1 számot.

A jelszavakat 60 naponta kötelező megváltoztatni.

A rendszergazdai jogosultsággal rendelkező felhasználók felhasználó nevüket és jelszavukat zárt borítékban kötelesek elhelyezni az Intézményvezető páncélszekrényében.

ADATBIZTONSÁG

Az archivált adatokat, és a biztonsági mentéseket, azonos biztonsági szinten kell kezelni, mint a használatban lévő adatokat, nyilvántartásokat.

A mentésekhez használt berendezéseket, eszközöket, informatikai „ürességi” vizsgálat nélkül, selejtezni, értékesíteni tilos.

MUNKAÁLLOMÁSOK VÉDELME

A munkaállomásokon egyedi vírusvédelmi szoftvereket kell futtatni. A szoftver beállítása és frissítése egyedileg történik.

A munkaállomásokat jelszóval kell védeni.

A képernyővédőt jelszóval kell védeni. A képernyővédőt automatikusan aktiválni kell 10 perc inaktivitás után.

A munkaállomások merevlemezei csak a rajta található adatok végleges és biztonságos megsemmisítését követően selejtezhetők. Az adatok megsemmisítéséről jegyzőkönyvet kell felvenni.

HORDOZHATÓ ESZKÖZÖK VÉDELME

A felhasználók által használt hordozható eszközök (pendrive, hordozható merevlemez) biztonságos tárolásáért, lopás és elvesztés elleni védelméért a felhasználó felel.

A hordozható eszközökre érzékeny, személyes, titkos adatot másolni tilos a meghajtó teljes titkosítása nélkül!

Hordozható eszközök csak a rajta található adatok végleges és biztonságos megsemmisítését követően selejtezhetők. Az adatok megsemmisítéséről jegyzőkönyvet kell felvenni.

3.1.1.1.3.6. AZ EMBERI ERŐFORRÁSOKBAN REJLŐ VESZÉLYEK MEGAKADÁLYOZÁSA

Az emberi erőforrás rosszhiszemű és nem rosszhiszemű tevékenysége miatti károk megelőzése, ill. a károk hatásának minimalizálása érdekében védelmi intézkedéseket kell bevezetni a munkavégzés minden fázisában. Az emberi erőforrások védelme során figyelembe kell venni a hatályos jogszabályokat, szabályzatokat, eljárásrendeket.

A munkavégzés csak akkor folytatható, ha a munkatárs megismerte a vonatkozó informatikai biztonsági szabályzatokat és erről írásban nyilatkozott. Törekedni kell arra, hogy a munkatársak informatikai biztonsági képzettsége és tudatossága folyamatosan fejlődjön. Az e területen megtett intézkedéseket dokumentálni kell (képzési napló)

A vezetőknek minden szinten feladata az informatikai biztonsági követelmények, eljárások működésének elvárása, betartatása és ellenőrzése. Az informatikai biztonsági követelmények megszegése esetén az alkalmazott fegyelmi eljárást és az alkalmazott szankciók részleteit rögzíteni kell.

Munkatársak munkaviszonyának megszűnése, változása esetén a munkatárssal a közvetlen vezető átadás-átvételi megállapodást köt, mely tartalmazza a felelősségek, feladatok, a munkatárs által kezelt információk átadását. A megállapodás rögzíti az átadás ütemtervét, a hozzáférések megszűntetését, az eszközök visszaadását, visszavételét, az esetleges átmeneti intézkedéseket. A hozzáférések megszüntetéséért a közvetlen vezető felelős.

3.1.1.1.3.7. AZ INFORMATIKAI BIZTONSÁG TUDATOSÍTÁSÁRA IRÁNYULÓ KÉPZÉS

A KÉPZÉSEK CÉLJA

Az Információ biztonsági képzések alapvető célja a munkatársak, és a szabályzat hatálya alá tartozók ismereteinek bővítése, frissítése.

A KÉPZÉSEKKEL SZEMBENI ELVÁRÁSOK, KÉPZÉSEK FAJTÁI

A képzésekkel szemben céljuk szerint az alábbi elvárások fogalmazhatóak meg:

BETANÍTÓ KÉPZÉS:

Célja az új vagy áthelyezett felhasználó megismertetése a rendszerrel, és az informatikai szabályokkal, a képzést egyénileg vagy csoportosan lehet megtartani.

SZINTEN TARTÓ KÉPZÉS:

Célja az ismeretek felfrissítése, a jogszabályváltozások követése, a technikai változások megismerése. A képzés anyaga épülhet a Szervezetben tapasztalt események elemzésére.

FEJLESZTŐ KÉPZÉSEK:

Az információbiztonság témakörére épített tréning jellegű képzés, az elvárt magatartások begyakorlása, és a várható események kezelése, az oktatási anyag része. A képzés irányulhat a technikai változások beillesztésére való felkészülésre, a logikai változások tanulmányozására.

A KÉPZÉS TÉMAKÖREI

A képzésen a következő témaköröket kell minimálisan érinteni:

a) Információbiztonsági alapfogalmak;
b) Támadási formák:
c) számítógépes kártevők fajtái;
d) ember által elkövetett támadások fajtái;
e) Vonatkozó jogszabályok, szabályzatok;
f) Felhasználók feladatai, felelőssége és jogai;
g) Biztonsági események felismerése és jelentése;
h) Az Internet és az elektronikus levelezés biztonsága;
i) Vírusok és egyéb kártevők elleni védelmi intézkedések;
j) A Helpdesk rendszer használata;
k) Jogosultsági rendszer, jogosultság igénylés folyamata;

3.1.1.1.3.8. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI BEÁLLÍTÁSÁVAL KAPCSOLATOS FELADATOK, ELVÁRÁSOK, JOGOK

Az informatikai eszközök szakszerű konfigurálása kizárólag az üzemeltetésre jogosult külső, illetve belső alkalmazottak feladata.

Az erre felhatalmazással nem rendelkezők számára a határvédelmi berendezése, szoftverek beállításainak megváltoztatása szigorúan tilos!

Az eszközök, illetve szoftverek ki és bekapcsolása szintén engedélyhez kötött, még abban az esetben is, ha a cselekmény csak időszaki működési szünetet okoz.

A biztonsági rendszerek működésében felfedezett bárminemű változást, az azt felfedező köteles haladéktalanul jelenteni az Informatikai Biztonsági Felelősnek, és az üzemeltetésre jogosultnak.

A beállításokhoz, illetve az üzemeltetéshez kapcsolódó jogosultságok kiosztására, illetve megváltoztatására az Informatikai Biztonságért felelős felsővezető, illetve meghatalmazottja jogosult.

3.1.1.1.3.9. ÜZEMMENET FOLYTONOSSÁG TERVEZÉSE

Az üzletmenet folytonosság tervezési folyamatában az első lépés, az elsődleges szolgáltatások meghatározása (alapszolgálatatások). Az alapszolgátatási kötelezettségekről külön törvények rendelkeznek. Meg kell határozni a szolgáltatások szüneteléséhez kapcsolódó tűrési képességet is, ami megmutatja, hogy az adott informatikai rendszer kiesése esetén a működés meddig tartható fent. Meg kell határozni, a tűrési képesség határnapjain indítandó tartalékszolgáltatásokat, és az ehhez kapcsolódó feladatokat, felelősségeket.

3.1.1.1.3.10. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK KARBANTARTÁSÁNAK RENDJE

Az informatikai rendszerek folyamatos, és megbízható működésének fenntartásához, karbantartási tervet kell készíteni, minden évre vonatkozóan. A tervnek megfelelően kell biztosítani a rendszer szoftver és hardverelemeinek előírt időszakonként szakszerű karbantartását.

A szerverek és az ezeken futó szoftverek, határvédelmi rendszerek karbantartása az üzemeltetők feladata. A felhasználók által használt eszközök tisztántartása, állagmegóvása a felhasználó kötelezettsége.

A külső felek által végzett karbantartási munkák engedélyhez kötöttek, ezeket az üzemeltetés felügyeletével megbízott vezető adhatja.

A karbantartások folyamán lehetőség szerint kerülni kell az eszköz fizikai helyének változtatását.

3.1.1.1.3.11. AZ ADATHORDOZÓK FIZIKAI ÉS LOGIKAI VÉDELMÉNEK SZABÁLYOZÁSA

Az archív állományokat tartalmazó adathordozókat, nyilván kell tartani, az alábbi adatok megjelölésével:

- Milyen adat található rajta
- Mentés ideje
- Meddig őrizhető
- Személyes adatok jelenléte
- Tárolási helye
- Sorszáma

Az archivált adatokat, és a biztonsági mentéseket, azonos biztonsági szinten kell kezelni, mint a használatban lévő adatokat, nyilvántartásokat.

A mentésekhez használt berendezéseket, eszközöket, informatikai „ürességi” vizsgálat nélkül, selejtezni, értékesíteni tilos.

3.1.1.1.3.12. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZERHEZ VALÓ HOZZÁFÉRÉS SORÁN KÖVETENDŐ AZONOSÍTÁSI ÉS HITELESÍTÉSI ELJÁRÁS, ÉS A HOZZÁFÉRÉSI SZABÁLYOK BETARTÁSÁNAK ELLENŐRZÉSE

Az informatikai rendszernek azonosítania és hitelesítenie kell a felhasználóit, és a felhasználók által végzett tevékenységeket.

A rendszerekhez történő hozzáférésekhez, egyénekhez kötött azonosítókat kell alkalmazni.

A csoportos azonosítók alkalmazása tilos, amennyiben bármely azonosító bizalmasságának sérüléséről informálódik a szabályzat hatálya alá tartozó felhasználó, azt az IBF-nek haladéktalanul jelenteni köteles.

3.1.1.1.3.13. A RENDSZEREK HASZNÁLATÁRÓL SZÓLÓ RENDSZERBEJEGYZÉSEK ÉRTÉKELÉSE, AZ ÉRTÉKELÉS EREDMÉNYÉTŐL FÜGGŐ ELJÁRÁSOK MEGHATÁROZÁSA

Az informatikai rendszerek használatáról naplóbejegyzéseket kell keletkeztetni. A bejegyzéseknek közvetlenül, vagy közvetett módon alkalmasnak kell lennie, hogy meghatározzák:

a) A belépő egyedi azonosítóját
b) A belépés idejét
c) A kilépés idejét
d) A használat során módosított adatokat tételesen
e) A használat közben párhuzamosan futtatott alkalmazásokat

Amennyiben a naplóállományok felülvizsgálatakor rendellenes tevékenységre utaló jelet tapasztal a felülvizsgálatot végző személy, az elérések felfüggesztése mellett, azonnal köteles gondoskodni a szükséges biztonsági eljárás megindításáról.

NAPLÓZÁSI ELJÁRÁSREND

A biztonságos üzemeltetés alapfeltétele a naplózás, a jelenlegi hálózati környezetben az alapértelmezett naplózási tevékenysége az operációs rendszerek végzik. A Szervezet törekszik rá, hogy lehetőségeinek függvényében naplózás elemző szoftvereket vásároljon, üzemeltessen, hiszen minél áttekinthetőbb riportokat kap a hálózati tevékenységekről annál pontosabban képes „finom hangolni" üzemeltetési, ellenőrzési tevékenységét. A jelenlegi rendszerben kiolvasott és személyes adatoktól megtisztított log elemzését az Informatikai biztonsági felelős elvégzi, megállapításait jegyzőkönyvbe foglalja. Az eljárásrend részletes leírása a Logikai Szabályzatban található.

3.1.1.1.3.14. AZ ADATOK MENTÉSÉNEK, ARCHIVÁLÁSÁNAK RENDJE

A hálózati merevlemezeken található adatok és beállítások rendszeres mentése a rendszergazdák feladata.

A munkaállomásokon található adatok rendszeres mentése a felhasználó feladata.

Az adatok mentése független adattárolóra történik. A kiemelten fontos adatok a szervezeti vezető, vagy az informatika egyedi döntése alapján optikai adathordozóra is menthetők, de ebben az esetben legalább 2 másolatot kell készíteni.

A mentéseket a következő mentési terv alapján kell elvégezni:

Iktató rendszer: Naponta

Ügyviteli rendszerek: Naponta

Felhasználói adatok: Hetente

A munka során keletkező minden adatot a kialakított könyvtárstruktúrában kell tárolni, ez alól felmentést csak az Informatikai vezető adhat.

AZ ADATTÁROLÁS BEMUTATÁSA

A felhasználók elsősorban az általuk használt munkaállomás tároló egységein rögzítik adataikat.

Egyes kollégáknak más hálózati meghajtók is megjelenhetnek a gépükön, ami általában a munkájukhoz szükséges speciális szoftverekhez szükséges (Pl. X:\ Csatorna vagy Z:\Utasitasok, Y:\E-Szigno)

LOKÁLIS FELHASZNÁLÓI KÖNYVTÁRAK

Minden felhasználó személyes könyvtára, ahol a munkájával kapcsolatos adatokat tárolhatja. A könyvtárban nem tárolhatók olyan adatok, amelyeken több személy dolgozik, vagy amelyekről munkáltatója úgy dönt, hogy azt más könyvtárában kell tárolni.

HÁLÓZATON KÍVÜLI MUNKA

A hordozható számítógépet használó felhasználók esetében szükséges a hálózati tárolási helyek és a merevlemez egyes részeinek szinkronizálása.

A munkaállomásra mentett adatokat a számítógép következő csatlakozásakor automatikusan szinkronizálja a háttérben a megfelelő hálózati helyre.

3.1.1.1.3.15. A BIZTONSÁGI ESEMÉNYEK ELJÁRÁSRENDJE

A biztonsági események olyan események, melyek eltérnek a megszokott ügymenettől, zavarokat okozhatnak és fenyegethetik az információk, illetve az információ feldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

Minősített incidens a hibás működés, mely a rendszerelemek (hardverek, szoftverek, adathordozók) rendeltetésszerű használata közben fellépő, normál működéstől eltérő működését jelenti.

Elsődleges szabály, hogy az információbiztonsági incidensek gyanújának felmerülésekor (incidens észlelésekor) azonnal értesíteni kell a jelentési kötelezettségnél meghatározott felelőst. TILOS az incidens körülményeit vizsgálni, illetve megkísérelni, elhárítani azt.

3.1.1.1.3.16. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZERHEZ -KÜLSŐ FELEK ÁLTALI- HOZZÁFÉRÉSÉNEK FELTÉTELEI

A külső fejlesztésekre, és hozzáférésekre vonatkozó szerződéseknek, ill. a szerződésekhez tartozó műszaki specifikációknak, ill. a fejlesztési projektekhez tartozó megállapodásoknak ki kell térniük az IT biztonsági követelményekre és azokra az átadás-átvételi feltételekre, amelyek alapján ezek ellenőrzésre kerülnek.

A fejlesztés tervezése során az IT biztonsági követelményeket a fejlesztésért felelős az IT biztonságért felelős vezetővel együttműködve azonosítja, és illeszti a specifikációba. meghatározzák, hogy a rendszer működése során milyen bemenő adat ellenőrzési, feldolgozás ellenőrzési, titkosítási, üzenet sértetlenség ellenőrzési, kimenő adat ellenőrzési követelmények fogalmazódnak meg, és a kapcsolódó követelményeket szintén beépítik a specifikációba. A specifikációt elfogadás előtt írásban véleményezi az IT biztonságért felelős vezető.

Amennyiben külső fejlesztők működnek közre a fejlesztésben, a fejlesztéshez kijelölt projektvezető feladata az információ kiszivárgás kockázatának csökkentése és a fejlesztőkkel együttműködés során a biztonsági követelmények betartása, betartatása. E célból együtt kell működnie az IT biztonságért felelős vezetővel.

Annak érdekében, hogy az informatikai rendszereknek a biztonság szerves részét képezze, a biztonsági követelményeket már az életciklus tervezési, fejlesztési, beszerzési szakaszában figyelembe kell venni. Az üzemeltetés és karbantartás során az információbiztonsági követelményeket folyamatosan fenn kell tartani.

3.1.1.1.4. A BIZTONSÁGI SZINT, VALAMINT AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK ELVÁRT BIZTONSÁGI OSZTÁLYAINAK MEGHATÁROZÁSA.

A biztonsági szint és az alkalmazások biztonsági osztályainak meghatározásához, a Nemzeti Kibervédelmi Intézet (NKI) által közzétett és honlapján elérhető „Osztályba Sorolás és Védelmi intézkedés űrlap” specifikációit kell igénybe venni. A besorolási segédlet az IBSZ elektronikus melléklete.

A kockázatarányos, költséghatékony védelem megvalósítása érdekében az Ibtv. alapján a Szervezet informatikai rendszereit biztonsági osztályba, illetve a Szervezetet – illetve az informatikai rendszerek fejlesztését végző,

üzemeltetését végző, üzemeltetéséért felelős vagy információbiztonságáért felelős szervezeti egységeket külön is – biztonsági szintbe kell sorolni.

Az informatikai rendszereket külön-külön kell 1-től 5-ig terjedő skálán biztonsági osztályba sorolni bizalmasság, sértetlenség és rendelkezésre állás szempontjából, ezek elvesztéséből fakadó jogi, társadalmi-politikai, közvetlen és közvetett anyagi kár vagy hatás alapján.

A szervezet vagy szervezeti egységek biztonsági szintjének 1-től 5-ig terjedő skálán történő meghatározását az informatikai rendszerek felhasználásának módja határozza meg.

A biztonsági osztály számozásának emelkedése egyre szigorodó védelmi előírásokat jelent és meghatározza, hogy az IBSZ mely rendelkezései vonatkoznak egy adott informatikai rendszerre.

A biztonsági osztályba és biztonsági szintbe sorolás részletes útmutatóját az Ibtv-hez kapcsolódó technológiai végrehajtási rendelet tartalmazza.

A biztonsági osztályba és szintbe sorolást az IBF készíti elő és az informatikai vezető hagyja jóvá.

A besorolás eredményét dokumentált módon legalább háromévente, de a következő esetekben soron kívül felül kell vizsgálni:

f) új informatikai rendszer kerül bevezetésre;
g) változás áll be a Szervezet státuszában;
h) változás következik be a Szervezet által kezelt vagy feldolgozott adatok vonatkozásában;
i) változik az informatikai rendszerek biztonságát érintő jogszabály.

Az elvégzett besorolás az eredményét külön mellékletek rögzítik.

Ha a Szervezet az informatikai rendszerek biztonsági osztályba sorolásánál hiányosságot állapít meg, vagy a szervezet/szervezeti egység biztonsági szintjének meghatározásánál a jelenleg teljesített biztonsági szint alacsonyabb, mint az előírt biztonsági szint, akkor a hiányosságok megszüntetése, illetve az előírt biztonsági szint elérésére érdekében *Intézkedési tervet* kell kidolgozni.

3.1.1.2. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS SZEMÉLY

A Szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 13. §-ában meghatározott feladatokat.

A védelem megfelelő szakmai szinten és korszerűen tartása az Informatikai biztonsági felelős (IBF) feladata. Az informatikai biztonsági felelős kijelölésének módjáról, és idejéről az Intézményvezető dönt.

3.1.1.2.1. AZ INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS SZEMÉLY FELADATAI

Az IBF jogosultságairól a feladatok és felelősségek fejezetben rendelkezett a szervezet, melynek a 2013. évi L. törvény rendelkezéseivel összhangban kell lennie.

3.1.1.3. AZ INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEI

Az intézkedési tervet a szükséges intézkedések végrehajtásáért felelős személyek és a vonatkozó határidők megjelölésével kell elkészíteni vonatkozó eljárási szabályok, felelősök, határidők megjelölésével.

A Szervezetnek *Intézkedési tervet* kell készítenie az alábbi esetekben:

a) az informatikai rendszerek biztonsági osztályba sorolásánál megállapított hiányosságok megszüntetésére; vagy a szervezet/szervezeti egység előírt biztonsági szintjének elérése érdekében, ha a jelenleg teljesített biztonsági szint az előírttól alacsonyabb
b) a kockázatelemzés és az esetleges biztonsági auditok során feltárt biztonsági kockázatok csökkentésére a *Kockázatkezelési terv* formájába
c) a bejelentett vagy a biztonsági események vizsgálata, illetve az IBSZ betartásának ellenőrzése feltárt biztonsági hibák javítására.

Az *Intézkedési tervben* rögzíteni kell az alábbiakat:

d) a megvalósítandó intézkedéseket;
e) a feladatok végrehajtásának becsült munkaidő ráfordítását és az esetleges költségeket;
f) a feladatok mellé rendelt felelőst;
g) a feladatok végrehajtásának határidejét.

A tervet az IBF javaslatainak figyelembevételével az informatikai vezető irányításával és a rendszergazda közreműködésével kell kidolgozni. A biztonsági kockázatok, biztonsági hibák vagy hiányosságok feltárását követően a terv elkészítésére a biztonsági osztályba vagy szintbe sorolás során feltárt hiányosságok esetén 90 nap áll rendelkezésre.

A terv végrehajtását a Szervezet vezetője hagyja jóvá.

3.1.1.3.1.1. AZ INTÉZKEDÉSI TERV MÉRFÖLDKÖVEI

Az intézkedési tervben az egyes feladatokhoz kapcsolódó határidőket úgy kell meghatározni, hogy azok számon kérhetőek legyenek. Amennyiben a feladat jellege egy éven túl mutat, akkor részfeladatokat, illetve részhatáridőket kell meghatározni, abban az esetben, ahol ez értelmezhető.

Ellenőrzési pontok és felelős személyek megnevezése alapvető elvárás.

3.1.1.3.1.2. AZ INTÉZKEDÉSI TERV FELÜLVIZSGÁLATA

Az intézkedési terv elkészítéséért, végrehajtásáért, felülvizsgálatáért és a megtett intézkedésekről a szervezet vezetőjének történő beszámolásért az IBF a felelős.

Az *Intézkedési tervet/Kockázatkezelési tervet* 90 naponként felül kell vizsgálni és a változásoknak megfelelően karban kell tartani.

3.1.1.3.1.2.1. A KOCKÁZATKEZELÉSI STRATÉGIA

A feltárt kockázatokat, a módszertanban meghatározott módon kell kezelni, illetve priorizálni. Külső tanúsító által feltárt kockázatok esetén kockázatok tanúsító által történő besorolása az iránymutató.

3.1.1.3.1.2.2. FELÜLVIZSGÁLAT

Ha az adott elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál az IBF hiányosságot állapít meg, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, a hiányosság megszüntetése érdekében.

3.1.1.3.1.2.3. A BIZTONSÁGI SZINT ELÉGTELENSÉGE

Ha a meghatározott biztonsági szint alacsonyabb, mint az elvárt szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, az előírt biztonsági szint elérése érdekében.

3.1.1.3.1.3. AZ INTÉZKEDÉSI TERV AKTUALIZÁLÁSA

Az IBF folyamatosan aktualizálja az intézkedési tervet.

3.1.1.4. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSA

Az tájékoztatásos rendszerek nyilvántartásának meg kell felelnie a 2013.évi L. törvény előírásainak, kerülni kell a könyvelési szempontú nyilvántartások használatát.

INFORMATIKAI ESZKÖZÖK KATEGÓRIÁI

A Szervezet informatikai eszközei a következő kategóriákba vannak besorolva.

a) Alkalmazások.
b) Szoftverek.
c) Szerverek.
d) Hálózati aktív elemek.
e) Hálózatok.
f) Felhasználói munkaállomások.
g) Nyomtatók, szkennerek.
h) Egyéb berendezések.

3.1.1.4.1.1. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSI MÓDJA

A rendszereket elegendő elektronikus formában nyilvántartani, a nyilvántartás az IBSZ kötelező melléklete.

Az egységes szabályozás érdekében – a Szervezet tevékenységét közvetlenül támogató, alkalmazói informatikai rendszerek (pl.: pénzügyi-számviteli rendszer, anyagrendszer, iktatórendszer, stb., továbbiakban: alkalmazói rendszerek) mellett – az alkalmazói szoftverek működéséhez szükséges környezet elhatárolható részeit, az alap informatikai szolgáltatásokat (pl.: központi címtár, fájl szerver szolgáltatások, levelező rendszer, stb.) megvalósító rendszereket is egy-egy informatikai rendszernek tekintjük (továbbiakban: alaprendszer).

Az informatikai vezető felelőssége, hogy felmérje a Szervezet informatikai rendszereit és kijelölje a rendszerek felett az Üzemeltető részéről felügyeletet gyakorló személyeket (a rendszergazdákat és helyettesüket), és előkészítse az *Informatikai rendszerek nyilvántartását*.

A kijelölt rendszergazdák feladata, hogy a felügyelt rendszerek nyilvántartott adatait feltöltsék, folyamatosan naprakészen tartsák, és évente felülvizsgálják.

A nyilvántartásnak minden rendszerre nézve minimálisan tartalmaznia kell:

a) a rendszer (és ha értelmezve van moduljának) megnevezését;
b) a rendszer állapotát (pl.: bevezetés alatt, éles, archív);
c) a rendszer rövid leírását (alapfeladatait, biztosítandó szolgáltatásokat);
d) az adatgazdai területet és vezetőjének nevét;
e) az adatgazdai terület részéről a rendszerben kezelt adatokért felelős kulcsfelhasználó és helyettesének nevét és elérhetőségét;
f) a rendszer felett felügyeletet gyakorló rendszergazda és helyettesének nevét és elérhetőségét;
g) a rendszert szállító/fejlesztő/karbantartó szervezetek nevét és elérhetőségét, valamint az illetékes kapcsolattartó személyek nevét és elérhetőségét;
h) van-e a rendszer követésére/karbantartására/támogatására vonatkozó szerződés (ha igen, a szerződés szkennelt változatát);
i) a rendszerekhez tartozó szoftverlicenceket és jellemzőit: típusát (vásárolt, bérelt, belső/külső fejlesztés, ingyenes), lejáratát (örökös, adott időszakra szóló), a licencet bizonyító dokumentum (számla, szállítói szerződés, licencszerződés) szkennelt változatát;
j) hardverrel együtt lett-e a rendszer vásárolva (ha igen, mivel);
k) a rendszer telepítésének helyét.

Az informatikai rendszerek bevezetési folyamatának részeként az *Informatikai rendszerek nyilvántartását* ki kell egészíteni az új rendszerekkel.

A nyilvántartás vezetését az IBF évente ellenőrzi.

A nyilvántartáshoz szorosan kapcsolódik és a rendszer dokumentációjának része az *Alapkonfiguráció* (ld. és a *Rendszerelem leltár*.

3.1.1.4.1.2. A NYILVÁNTARTÁSOK AKTUALIZÁLÁSA

A nyilvántartásokat tartalmi változásuk esetén azonnal, de legalább évente kell felülvizsgálni. A felülvizsgálatról nem kell külön jelentést készíteni, csak ha feloldhatatlan ellentmondást tár fel az eljárás.

3.1.1.4.2. A NYILVÁNTARTÁS TARTALMI ELEMEI

A nyilvántartásnak tartalmaznia kell:

- A rendszer:
    a. Megnevezését
    b. Moduljait
    c. Alapfeladatát
    d. Licenszeit
    e. Adatgazdáját/rendszergazdáját
    f. Beszállítóját
- A beszállítók:
    g. Hivatalos nevét
    h. Adószámát
    i. Címét
    j. Telefonszámát
    k. Mailcímét
    l. Kapcsolattartóját
- A felelősök:

m. Nevét
n. Munkáltatóját
o. Telefonszámát
p. Mailcímét

ESZKÖZÖK NYILVÁNTARTÁSA

Önállóan működő nagy értékű eszközök (monitorok, szünetmentes tápegységek, aktív eszközök)

a) tételazonosító sorszám;
b) az eszköz neve
c) az eszköz sorozat- vagy gyári száma
d) az eszköz státusza (használatban, raktáron, szervizben stb.)

Számítógépek

a) tételazonosító sorszám;
b) az eszköz neve
c) az eszköz sorozat- vagy gyári száma
d) az eszköz státusza (használatban, raktáron, szervizben stb.)
e) OEM operációs rendszer

3.1.1.4.2.1. ALAPFELADATOK

Minden alkalmazott rendszer esetében meg kell határozni annak alapfeladatait, és az alapfeladatokhoz kapcsolódó szerepköröket.

3.1.1.4.2.2. A RENDSZEREK ÁLTAL BIZTOSÍTANDÓ SZOLGÁLTATÁSOK

A fizikai és logikai rendszerek esetében meg kell határozni az azok által biztosított és igénybe vett szolgáltatásokat. Ezeket a megállapításokat a rendszerek dokumentációjában kell tárolni. A feladat felelőse a rendszer adatgazdája, vagy rendszergazdája.

3.1.1.4.2.3. LICENC SZÁMOK

Ha azok a szervezet kezelésében vannak licenszszámok, akkor azokat külön nyilvántartásban kell rögzíteni. Biztosítani kell, hogy a rendszerek telepítésért felelős személyek ezekhez igény szerint hozzáférjenek.

SZOFTVEREK NYILVÁNTARTÁSA

A nyilvántartás elemei:

a) tételazonosító sorszám;
b) a szoftver gyártója;
c) a szoftver neve;
d) a szoftver verziószáma;
e) a szoftver leírása;

f) a szoftver azonosító sorszáma, szériaszáma;
g) a szükséges hardver környezet;
h) a szükséges operációs rendszer, szoftverkörnyezet;
i) a licensz feltételei: Kik, hányan, hány számítógépen, mettől, meddig használhatják;
j) a szoftver típusa (OEM, frissítés);
k) ezen szoftver alapján frissített szoftver tételazonosítójának sorszáma;
l) a dokumentációt, illetve az eredeti adathordozót birtokló szervezeti egység megnevezése

EGYÉB ADATBÁZISOK NYILVÁNTARTÁSA

A nyilvántartás elemei:

a) tételazonosító sorszám;
b) az adatbázis vagy adat készítője;
c) az adatbázis vagy adat neve;
d) az adatbázis vagy adat verziószáma;
e) az adatbázis vagy adat leírása;
f) a dokumentációt, illetve az eredeti adathordozót birtokló szervezeti egység megnevezése

3.1.1.4.2.4. A RENDSZER FELETT FELÜGYELETET GYAKORLÓ SZEMÉLY ADATAI

A rendszerek felügyeletét ellátó személyeknek nyilván kell tartani a személyazonosító és elérhetőségi adatait, ez a nyilvántartás az informatikai rendszerek nyilvántartásának a része.

3.1.1.4.2.5. A RENDSZERT SZÁLLÍTÓ, FEJLESZTŐ ÉS KARBANTARTÓ SZERVEZETEK AZONOSÍTÓI

A rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

3.1.1.5. AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS ENGEDÉLYEZÉSI ELJÁRÁS

Amennyiben az informatikai rendszerek környezetében, a biztonságot érintő változás következne be, a változást megelőzően engedélyezni kell a beavatkozást. A változtatást a terület rendszergazdája és az IBF együttesen engedélyezi.

3.1.1.5.1. AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS ENGEDÉLYEZÉS HATÓKÖRE

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, a Szervezet hatókörébe tartozó rendszerre.

A jogosultságok engedélyezését/kiosztását végző személynek törekednie kell a legkisebb jogosultság kiosztásához a felhasználók körében. A jogosultságok kiosztásánál javasolt figyelembe venni a szervezeti és működési szabályzatot. Az

indokoltnál magasabb hozzáférések (különösen a privilégiumokkal járó jogosultságok) kiadásának okát írásban kell rögzíteni. Az esetleges biztonsági események kivizsgálása során a jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán.

3.1.1.5.1.1. EMBERI, FIZIKAI ÉS LOGIKAI ERŐFORRÁSRA

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, a hatókörébe tartozó erőforrásra.

Az emberi erőforrás rosszhiszemű és nem rosszhiszemű tevékenysége miatti károk megelőzése, ill. a károk hatásának minimalizálása érdekében védelmi intézkedéseket kell bevezetni a munkavégzés minden fázisában. Az emberi erőforrások védelme során figyelembe kell venni a hatályos jogszabályokat, szabályzatokat, eljárásrendeket.

Az alkalmazás informatikai biztonsági feltételeit a munkaszerződéseknek (vállalkozói együttműködés esetén az vállalkozói szerződés), és a munkaköri leírásoknak is tartalmazniuk kell. A munkatársak kiválasztási folyamatában az alkalmazási feltételek között szerepeltetni kell az informatikai biztonsági követelményeket is.

A munkavégzés csak akkor kezdhető meg, ha a munkatárs megismerte a vonatkozó informatikai biztonsági szabályzatokat és erről írásban nyilatkozott. Törekedni kell arra, hogy a munkatársak informatikai biztonsági képzettsége és tudatossága folyamatosan fejlődjön. Az e területen megtett intézkedéseket dokumentálni kell (képzési napló)

A vezetőknek minden szinten feladata az informatikai biztonsági követelmények, eljárások működésének elvárása, betartatása és ellenőrzése. Az informatikai biztonsági követelmények megszegése esetén az alkalmazott fegyelmi eljárást és az alkalmazott szankciók részleteit rögzíteni kell.

Munkatársak munkaviszonyának megszűnése, változása esetén a munkatárssal a közvetlen vezető átadás-átvételi megállapodást köt, mely tartalmazza a felelősségek, feladatok, a munkatárs által kezelt információk átadását. A megállapodás rögzíti az átadás ütemtervét, a hozzáférések megszűntetését, az eszközök visszaadását, visszavételét, az esetleges átmeneti intézkedéseket. A hozzáférések megszüntetéséért a közvetlen vezető felelős.

3.1.1.5.1.2. AZ ELJÁRÁSI ÉS VÉDELMI KÖVETELMÉNYSZINT ÉS FOLYAMAT

Az engedélyezési eljárás folyamán figyelembe kell venni az adott rendszer besorolási eredményeit, követelményeit, a végrehajtási folyamat során a biztonsági körülmények nem lehetnek alacsonyabbak az elvártnál.

3.1.2.1. KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSREND

3.1.2.1.1.1. KIHIRDETÉSI SZABÁLYOK

A kockázatelemzés eredményének kihirdetése, azonos a szabályzat kihirdetésének rendjével.

3.1.2.1.1.2. FELÜLVIZSGÁLAT

A kockázatelemzés felülvizsgálata esedékes a rendszer bármely számottevő változtatása esetén, de legalább évente, március 31-ig.

3.1.2.1.2. AZ ELJÁRÁSREND TERJEDELME

Az eljárásrend kiterjed a módszer bemutatására, a kockázatelemzés megállapításaira, és a megállapítások értelmezésére.

3.1.2.1.2.1. A KOCKÁZATOK FELMÉRÉSE

A kockázatokkal kapcsolatos eljárásrend részletes leírását lásd a 3*.1.1.1.3.1. Kockázatelemzés* pontban

3.1.2.2. BIZTONSÁGI OSZTÁLYBA SOROLÁS

3.1.2.2.1.1. A BESOROLÁS

A Szervezet jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és a 3.1.1.4. pont szerinti nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók.

3.1.2.2.1.2. JÓVÁHAGYÁS

A szervezet vezetője kizárólagosan hagyja jóvá a biztonsági osztályba sorolást.

3.1.2.2.1.3. RÖGZÍTÉS

A biztonsági osztályba sorolás eredményét lásd az IBSZ mellékletében.

3.1.2.2.2. ELVÁRÁSOK

3.1.2.2.2.1. FELÜLVIZSGÁLAT

A biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten el kell végezni, de legalább évente.

3.1.2.2.2.2. A BESOROLÁS KAPCSOLÓDÁSA AZ INTÉZKEDÉSI TERVHEZ

Kapcsolódást kell biztosítani a 3.1.1.3. pontban foglalt intézkedési tervhez és mérföldköveihez.

3.1.2.3. KOCKÁZATELEMZÉS

A kockázatelemzés részletes szabályait rögzítettük a szabályzat „3.1.1.1.3.1. Kockázatelemzés” fejezetében, a módszertani leiratokban.

3.1.2.3.1.1. A BIZTONSÁGI KOCKÁZATELEMZÉSEK VÉGREHAJTÁSA

A kockázatelemzéseket évente rendszeresen, de a rendszereket érintő változások esetén haladéktalanul végre kell hajtani.

3.1.2.3.1.2. AZ EREDMÉNYEK RÖGZÍTÉSE

A kockázatelemzések eredményét a kockázatelemzési jelentésben, vagy a kockázatelemzési eljárásrendben előírt dokumentumban kell rögzíteni.

3.1.2.3.1.3. FELÜLVIZSGÁLAT

Az IBF a kockázatelemzési eljárásrendnek megfelelően felülvizsgálja a kockázatelemzések eredményét, erről a szervezeti vezetőket tájékoztatja.

3.1.2.3.1.4. NYILVÁNOSSÁG

A kockázatelemzési eljárásrendnek megfelelően, vagy a 3.1.1.1. pont szerinti informatikai biztonsági szabályzata keretében megismerteti a kockázatelemzés eredményét az érintettekkel. A tájékoztatás kizárólag a végrehajtásban nevesített személyek részére kötelező. A felmérés eredménye bizalmas!

3.1.2.3.1.5. FELÜLVIZSGÁLAT

Amikor változás áll be az elektronikus információs rendszerben külső környezetében, vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést kell végrehajtani a szabályzat „3.1.2.3.1.3. Felülvizsgálat” pontja szerint.

3.1.2.3.1.6. BIZALMASSÁG

Az IBF gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.

3.1.3.1. BESZERZÉSI ELJÁRÁSREND

A beszerzési eljárásrend az eszközök, és szolgáltatások beszerzéssel kapcsolatos szabályokat és feladatokat rögzítése.

3.1.3.1.1.1. KIHIRDETÉS

A szervezet, beszerzési eljárásrendjét külön szabályzatban rögzíti. Ebben megfogalmazza, és az érvényes követelmények szerint dokumentálja, valamint kihirdeti a beszerzési eljárásrendet, mely az elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg, és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő.

3.1.3.1.1.2. FELÜLVIZSGÁLAT

A szervezet a beszerzési eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a beszerzési eljárásrendet.

3.1.3.2. ERŐFORRÁS IGÉNY FELMÉRÉS

A rendszer működéséhez szükséges erőforrások felmérése a folyamatos munka során történik.

3.1.3.2.1.1. ERŐFORRÁSIGÉNY MEGHATÁROZÁSA

A szervezet az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként.

3.1.3.2.1.2. BIZALMASSÁG

Elkülönítetten kezeli az elektronikus információs rendszerek biztonságát beruházás tervezési dokumentumaiban, ezeket a rendelkezésére álló eszközökkel védi.

3.1.3.3. BESZERZÉSEK

3.1.3.3.1. A BESZERZÉSI KÖVETELMÉNYEK MEGHATÁROZÁSA

A Szervezet az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza az alábbiakat.

A Szervezet egységes, jól működő, költséghatékony informatikai rendszerének kialakításához és fenntartásához egy Informatikai Fejlesztési Stratégia elkészítése szükséges.

3.1.3.3.1.1. A FUNKCIONÁLIS BIZTONSÁGI KÖVETELMÉNYEK

A beszerzésre kerülő rendszerek az alapvető és más jogszabályokban megkövetelt működési elvárásait teljesítenie kell. Az érintett rendszer esetleges cseréje esetén gondoskodni kell az előzetes felkészülésről, hogy a korábban használt, illetve szükséges folyamatok az új rendszerben hogyan érhetőek el.

3.1.3.3.1.2. BIZTONSÁGI GARANCIÁK

A garanciális biztonsági követelmények.

- A beszerzésre kerülő rendszerek biztonsági funkciói nem gyengülhetnek sem az elvárások, sem a korábbi rendszer paramétereinek tekintetében.
- Figyelembe kell venni a változó jogszabályi előírásokat
- A beszerzést megelőzően nem adható ki „valós alapú” tesztadat
- Vizsgálni kell a termék előállítójának alkalmazott eljárásait, szabványait
- Az előzetes tesztelés kötelező

3.1.3.3.1.3. DOKUMENTÁCIÓS KÖVETELMÉNYEK

A biztonsággal kapcsolatos dokumentációs követelményeket, előzetesen meg kell fogalmazni. A rendszerrel kapcsolatosan alapvető elvárás, hogy a felhasználói, és a biztonsági dokumentáció különállóan jelenjen meg, és önállóan is értelmezhetőtek legyenek.

A fejlesztésekre vonatkozó szerződéseknek, ill. a szerződésekhez tartozó műszaki specifikációknak, ill. a fejlesztési projektekhez tartozó megállapodásoknak ki kell térniük az IT biztonsági követelményekre és azokra az átadás-átvételi feltételekre, amelyek alapján ezek ellenőrzésre kerülnek.

A fejlesztés tervezése során az IT biztonsági követelményeket a fejlesztésért felelős az IT biztonságért felelős vezetővel együttműködve azonosítja, és illeszti a specifikációba. meghatározzák, hogy a rendszer működése során milyen bemenő adat ellenőrzési, feldolgozás ellenőrzési, titkosítási, üzenet sértetlenség ellenőrzési, kimenő adat ellenőrzési követelmények fogalmazódnak meg, és a kapcsolódó követelményeket szintén beépítik a specifikációba. A specifikációt elfogadás előtt írásban véleményezi az IT biztonságért felelős vezető.

Minden egyedi fejlesztés esetén át kell venni és el kell tárolni a forráskódot és a fejlesztői környezetet.

A bevezetésre kerülő rendszereket bevezetés előtti tesztelni szükséges. A tesztelésnek ki kell térnie a bevezetés által érintett kapcsolódó rendszerek tesztelésére is. A tesztelések és a bevezetés során az IT üzemeltetésnek kell gondoskodnia arról, hogy éles rendszeren csak engedélyezett és felügyelt módosítás történhessen. Ugyancsak az IT üzemeltetésnek kell gondoskodnia arról, hogy a megfelelőség ellenőrzéséhez használt teszt adatokhoz, illetve a forráskódokhoz illetéktelen ne férjen hozzá.

Amennyiben külső fejlesztők működnek közre a fejlesztésben, a fejlesztéshez kijelölt projektvezető feladata az információ kiszivárgás kockázatának csökkentése és a fejlesztőkkel együttműködés során a biztonsági követelmények betartása, betartatása. E célból együtt kell működnie az IT biztonságért felelős vezetővel.

Annak érdekében, hogy az informatikai rendszereknek a biztonság szerves részét képezze, a biztonsági követelményeket már az életciklus tervezési, fejlesztési, beszerzési szakaszában figyelembe kell venni. Az üzemeltetés és karbantartás során az információbiztonsági követelményeket folyamatosan fenn kell tartani.

3.1.3.3.1.4. A DOKUMENTUMOK BIZALMASSÁGA

A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények alapvetően megegyeznek a rendszerrel szemben támasztott biztonsági követelményekkel.

3.1.3.3.1.5. A FEJLESZTŐI KÖRNYEZET

Az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozóan egyértelmű iránymutatással kell rendelkezni. A specifikációkat (hardver, szoftver elvárások) rögzíteni kell.

3.1.3.4. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZERRE VONATKOZÓ DOKUMENTÁCIÓ

3.1.3.4.1.1. ADMINISZTRÁTORI KÖVETELMÉNYEK

A rendszer üzemeltetése a Szervezet hatókörébe tartozik, ezért megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:

3.1.3.4.1.1.1. TELEPÍTÉSI DOKUMENTÁCIÓ

A rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését leíró adatokat, folyamatokat, specifikációkat.

3.1.3.4.1.1.2. BIZTONSÁGI FUNKCIÓK

A biztonsági funkciók hatékony alkalmazásának és fenntartásának leiratait.

3.1.3.4.1.1.3. Sérülékenységek

A konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket, gyengeségeket (kockázatelemzés, hatásvizsgálat)

3.1.3.4.1.2. FELHASZNÁLÓI KÖVETELMÉNYEK

A Szervezet megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza:

3.1.3.4.1.2.1. BIZTONSÁGI FUNKCIÓK

A felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját, ellenőrzését.

3.1.3.4.1.2.2. BIZTONSÁGOS HASZNÁLAT

A rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit.

3.1.3.4.1.2.3. A FELHASZNÁLÓ KÖTELEZETTSÉGEI

A felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához.

3.1.3.4.1.3. BIZALMASSÁG

A Szervezetnek gondoskodnia kell arról, hogy az információs rendszerre vonatkozó - különösen az adminisztrátori és fejlesztői - dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.3.4.1.4. RENDELKEZÉSRE ÁLLÁS

A Szervezet gondoskodik a dokumentációval meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

3.1.3.6. KÜLSŐ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI

3.1.3.6.1.1. A KÖVETELMÉNYEK MEGHATÁROZÁSA

A Szervezet szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az elektronikus információbiztonsági követelményeinek.

3.1.3.6.1.2. SZERVEZETI FELADATOK

A Szervezet meghatározza és dokumentálja a felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban.

3.1.3.6.1.3. ELLENŐRZÉS

A Szervezet külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

3.1.3.8. FOLYAMATOS ELLENŐRZÉS

3.1.3.8.1. AZ ELLENŐRZÉS TARTALMA

A Szervezet folyamatba épített ellenőrzést vagy ellenőrzési tervet hajt végre, amely tartalmazza:

3.1.3.8.1.1. AZ ELLENŐRZENDŐ TERÜLETEK

- Az informatikai eszközök és rendszerek használatának jogosultsága
- A jogosultságok szükségessége
- Adminisztrátori és felhasználói tevékenységek vizsgálata
- Frissítések, karbantartások megléte
- Előírt eljárások teljesítése
- Adminisztráció

3.1.3.8.1.2. GYAKORISÁG

Az ellenőrzések, negyedéves gyakorisággal valósulnak meg.

3.1.3.8.1.3. ÉRTÉKELÉS

Az ellenőrzéseket követően 60 napon belül összegző értékelést kell készíteni a tapasztalatokról.

3.1.3.8.1.4. A KONTROLLSZÁMOK

Lehetőség szerint az összegző eredményeket számszerűsíteni kell, figyelembe véve a szabványok ajánlásait.

3.1.3.8.1.5. ÖSSZEHASONLÍTÁS

Az értékelés folyamán, amennyiben az ellenőrzött területről már készültek korábbi felmérések összehasonlításokat kell végezni, a további intézkedések előkészítéséhez.

3.1.3.8.1.6. REAKCIÓ

Amennyiben az összehasonlító eredmények valamely területen a biztonsági képességek csökkenését mutatják, intézkedési tervet kell készíteni a korrekciós intézkedésekhez.

3.1.3.8.1.7. NYILVÁNOSSÁG

A Szervezet az ellenőrzések megállapításait legalább évente ismerteti az érintett személyekkel.

3.1.4.1. ÜZLETMENET-FOLYTONOSSÁGRA VONATKOZÓ ELJÁRÁSREND

Az *Üzletmenet-folytonossági tervben* meg kell határozni:

- a katasztrófa események definícióját;
- a terv életbe léptetésének a feltételeit (hogyan kell a helyzetet értékelni, kiket kell bevonni, ki dönti el a katasztrófa tényét, ki felelős a folyamat inicializálásáért);
- a vészhelyzeti szerepköröket, ezek felelősségét, feladatait;
- a szerepköröket betöltő személyek nevét és elérhetőségét;
- külső támogatást nyújtó partnerek esetén a kapcsolattartó személyek nevét és elérhetőségét;
- vészhelyzet esetén a szereplők értesítésének módját, a riadóláncot;
- mely informatikai rendszerek élveznek prioritást korlátozott vészhelyzeti működés esetén;
- az informatikai rendszerek alapfeladatait és alapfunkcióit (a biztosítandó szolgáltatásokat), a minimális funkcionalitást, amelyeket a rendszer összeomlása, kompromittálódása, vagy hibája ellenére is fenn kell tartani, valamint az alapfunkciókhoz kapcsolódó vészhelyzeti követelményeket;

- a vészhelyzet esetén követendő eljárásokat, azaz a működést és/vagy az emberi életet veszélyeztető esemény bekövetkezte után végzendő teendők leírását, beleértve a nyilvánosság kezelésére, a hatóságokkal (pl.: rendőrséggel, tűzoltósággal, önkormányzattal) történő hatékony kapcsolatfelvételre vonatkozó rendelkezéseket;
- az alapvető tevékenységek vészhelyzeti működésben történő folytatásának lehetőségeit, ezek megvalósításának lépéseit:
- az automatizált folyamatok kézi póteljárásait;
- az informatikai erőforrások dinamikus átcsoportosításának, tartalék eszközök beiktatásának a lehetőségét;
- idegen szervezet eszközeinek igénybevételére épülő tartalék megoldást;
- a felkészülési feladatokat a terv végrehajtásához, a biztosítandó erőforrásokat (pl.: a kézi póteljáráshoz szükséges törzs adatokat, szerződéseket stb.);

ÜZLETMENET FOLYTONOSSÁGI TERVEK KARBANTARTÁSA ÉS TESZTELÉSE

Az *Üzletmenet-folytonossági terv* elkészítéséért és karbantartásáért – a felhasználói oldal részéről a kulcsfelhasználókkal egyeztetve – az alkalmazásüzemeltetési és fejlesztési vezető, a *Katasztrófa elhárítási terv* elkészítéséért és karbantartásáért a rendszergazda a felelős. A tervek jóváhagyása az informatikai vezető, ellenőrzése az IBF feladata.

Az *Üzletmenet-folytonossági terv* és a *Katasztrófa elhárítási terv* bizalmas minősítésű dokumentumok, amelyeket a tervekben rögzített, a végrehajtásban érintett személyek, szervezeti egységek (vészhelyzeti szereplők) számára kell kihirdetni, akik illetékteleneknek nem adhatják tovább. A tervek megismerésére (és tárolására) jogosult vészhelyzeti szereplők feladata gondoskodni arról, hogy a terv jogosulatlanok számára ne legyen megismerhető, módosítható.

A terveket évente felül kell vizsgálni és minden olyan esetben aktualizálni kell, ha változás következik be az informatikai rendszerekben vagy környezetükben, illetve a tervekben szereplő adatokban, így például:

- új informatikai rendszer bevezetése;
- új nagyteljesítményű hardver eszközök beszerzése;
- a vészhelyzeti szereplők személyének változása;
- támogatást nyújtó külső partnerek változása;
- elérhetőségi adatok (e-mail címek, telefonszámok) változása.

A kidolgozott tervek végrehajtását évente tesztelni kell, ami biztosítja a naprakészség ellenőrzését. Az *Üzletmenet-folytonossági terv* teszteléséért a kulcsfelhasználó, a *Katasztrófa elhárítási terv* teszteléséért a rendszergazda a felelős. Ezekről a tesztekről írásos feljegyzést kell készíteniük.

A tervek éles helyzetben történő végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálni, javítani kell a tervek tartalmát.

A tervek változásairól tájékoztatni kell a tervekben rögzített vészhelyzeti szereplőket.

KATASZTRÓFA ELHÁRÍTÁSI TERV

A *Katasztrófa elhárítási tervben* meg kell határozni:

- a vészhelyzeti szerepköröket, ezek felelősségét, feladatait;
- a szerepköröket betöltő személyek nevét és elérhetőségét;
- támogatást nyújtó külső partnerek esetén a kapcsolattartó személyek nevét és elérhetőségét;
- a katasztrófa megelőzése érdekében végzett tevékenységeket;
- a katasztrófa elhárítás előfeltételeként elvégzendő mentések rendszerét;
- a felkészülési feladatokat a terv végrehajtásához, a biztosítandó erőforrásokat (pl.: tartalék- és segédeszközöket, telepítő adathordozókat, üzemeltetési dokumentációkat stb.);

- a végleges, teljes informatikai rendszer helyreállításának lépéseit úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket;

3.1.4.1.1.1. KIHIRDETÉS

A Szervezet megfogalmazza, és az érvényes követelmények szerint dokumentálja, valamint az érintett személyi kör részére kihirdeti az elektronikus információs rendszerre vonatkozó eljárásrendet, mely az üzletmenet-folytonosságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

3.1.4.1.1.2. FELÜLVIZSGÁLAT

A Szervezet az üzletmenet-folytonossági tervet, éves gyakorisággal felülvizsgálja és frissíti.

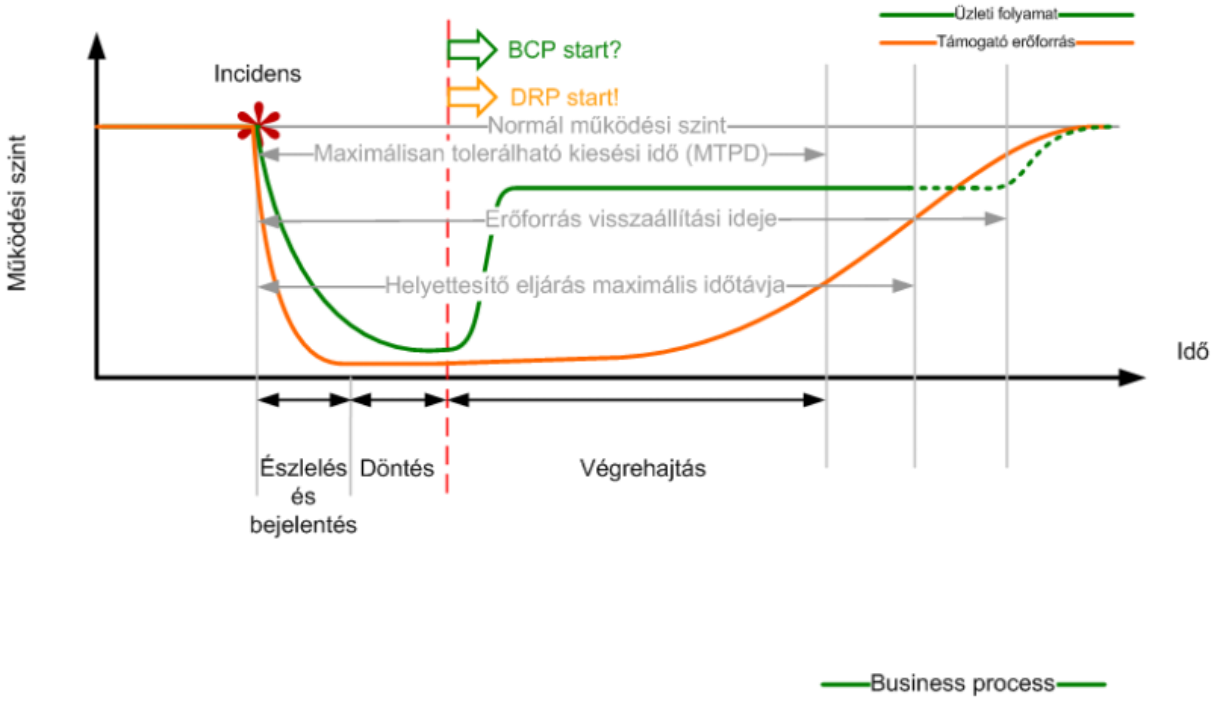
3.1.4.2. ÜZLETMENET-FOLYTONOSSÁGI TERV INFORMATIKAI ERŐFORRÁS KIESÉSEKRE

A Szervezetnek *Üzletmenet-folytonossági tervet* (BCP) és ezzel összefüggésben *Katasztrófa elhárítási tervet* (DRP) kell készítenie az informatikai erőforrások kiesésére vonatkozóan az informatikai rendszerek folyamatos működésének biztosításához.

Egy katasztrófa esemény, vészhelyzet bekövetkezésekor két folyamatot kell elindítani:

- egyrészt vissza kell állítani a katasztrófa következményeként kiesett informatikai erőforrásokat (erre vonatkozik a *Katasztrófa elhárítási terv*);
- másrészt biztosítani kell a rendszer teljes visszaállításáig a kiesett erőforrások nélküli minimális funkcionalitást nyújtó üzleti működést, vészhelyzeti működést (erről szól az *Üzletmenet-folytonossági terv*).

A *Katasztrófa elhárítási terv* minden esetben életbe lép, ha valamely, üzleti folyamatot támogató erőforrás kiesik. Az *Üzletmenet-folytonossági tervet* viszont csak akkor aktiválni, ha az erőforrás várható visszaállítási ideje meghaladja a meghatározott maximálisan tolerálható kiesési időt. Ha ezen belül vissza lehet állítani az erőforrást, akkor nincs szükség az *Üzletmenet-folytonossági terv* életbe léptetésére.



3.1.4.2.1.1. KIHIRDETÉS

A Szervezet megfogalmazza, és az érvényes követelmények szerint dokumentálja, valamint a Szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet.

3.1.4.2.1.2. ÖSSZEHANGOLÁS

A Szervezet összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével.

3.1.4.2.1.3. FELÜLVIZSGÁLAT

A Szervezet éves gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet.

3.1.4.2.1.4. AKTUALIZÁLÁS

A Szervezet az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően folyamatosan aktualizálja az üzletmenet-folytonossági tervet.

3.1.4.2.1.5. Nyilvánosság

A Szervezet tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket.

A dokumentum tartalmát megismerheti

- Intézményvezető
- rendszergazda (kliens és szerver oldali)
- adatgazda
- informatikai vezető (informatikai csoportvezető)
- információbiztonsági felelős
- érintett felhasználó Nyilvántartás szerintiek
- érintett szolgáltató Nyilvántartás szerintiek

3.1.4.2.1.6. BIZALMASSÁG

A Szervezet gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.4.2.1.7. ALAPFELADATOK MEGHATÁROZÁSA

A Szervezet elsődleges feladata a kormányzati és önkormányzati intézmények ellátó, kisegítő szolgálatai, ehhez nélkülözhetetlen rendszerek:

- közszolgálati rendszerek
- pénzügyi rendszerek
- nyilvántartási rendszerek

Az alapszolgáltatási kötelezettségekről külön törvények rendelkeznek, a rendszer tűrőképessége 30 nap, amennyiben ez idő alatt nem áll helyre a rendszer, az intézményvezető elrendeli az alternatív rendszer élesítését. Az alternatív rendszerek indításához, a felkészülést a 15 üzemszüneti napon kell megkezdeni.

3.1.4.2.1.8. HELYREÁLLÍTÁS

Amennyiben a közszolgálati rendszer a 15.-ik üzemszüneti napon sem működőképes, az alábbi lépéseket kell megtenni.

- A legutolsó sértetlen biztonsági mentés előkészítése átadásra (átadó rendszergazda)
- A biztonsági mentés bizalmasságának fenntartása (átadó IBF/ átvevő IBF)
- Az alternatív közszolgálati rendszer felkészítése (fogadó adatgazda)
- Az adatvédelmi bejelentések elkészítése a fogadó adatfeldolgozói tevékenységéről, és a feladatok elvégzéséhez szükséges szerződések megkötése (intézményvezető – adatvédelmi felelős)
- Az adatok átadása/átvétele (átadó adatgazda – fogadó adatgazda)
- Előzetes tesztelés (fogadó rendszergazda)
- A közszolgáltatási rendszer élesítése (átadó rendszergazda – átadó adatgazda)
- A szolgáltatás megkezdése (fogadó adatgazda)

3.1.4.2.1.9. SZEREPKÖRÖK, FELELŐSSÉGEK

A Szervezet első számú vezetője az

INTÉZMÉNYVEZETŐ

FELADATAI:

- Kinevezi, illetve megbízza az információbiztonsági felelőst (továbbiakban: IBF)
- Meghatározza az informatikai rendszerek védelmének felelőseire, feladataira, az ehhez szükséges hatáskörökre és a felhasználókra vonatkozó szabályokat, illetve kiadja az Informatikai Biztonsági Szabályzatot (továbbiakban: IBSZ).
- Biztosítja az IBSZ-ben megfogalmazott informatikai biztonsági szereplők részére a munkavégzésükhöz szükséges hatáskört és erőforrásokat.
- Biztosítja a Szervezet minden felhasználója számára a munkavégzéshez szükséges informatikai eszközöket és szoftvereket.
- Felelős a Szervezet informatikai rendszereinek kialakításáért, a fejlesztési feladatok meghatározásáért, valamint a rendszerek információbiztonságáért.
- Az IBF-fel rendszeresen ellenőrizteti, hogy a Szervezetnél megfelelően alkalmazzák-e az IBSZ előírásait.
- Egyszemélyi felelősségének megtartása mellett az egyes funkciók irányítását átadhatja más szervezeteknek és személyeknek.

INFORMATIKAI VEZETŐ (INFORMATIKAI CSOPORTVEZETŐ)

A Szervezet informatikai vezetője, az informatikával kapcsolatos feladatok koordinátora.

FELADATAI:

- Gondoskodik az informatikai biztonságra vonatkozó jogszabályok, a biztonságpolitika, a biztonsági stratégia és az IBSZ végrehajtásáról és betartásáról.
- Engedélyezi az információbiztonsággal kapcsolatos eljárási és védelmi követelményszinteket és folyamatokat.
- Felelős az informatikai rendszerek biztonságának folyamatos felülvizsgálatáért. Ennek keretében az IBF-fel elvégezteti az informatikai rendszerek kockázatelemzését.
- Felelős az informatikai rendszerek üzemeltetéséhez szükséges erőforrások biztosításáért és a rendszerek folyamatos működéséért. Gondoskodik a folyamatos munkát biztosító koordinációról és a zökkenőmentes végrehajtást akadályozó tényezők megszüntetéséről.
- Meghatározza az informatikai feladatok prioritását, végrehajtási sorrendjét.
- Felügyeli az alap informatikai szolgáltatásokat megvalósító alaprendszerek (pl. központi címtár, fájl szerver szolgáltatások, levelező rendszer stb.) és rendszerszoftverek (pl.: operációs rendszerek, adatbáziskezelő szoftverek, tűzfal szoftverek stb.), a szerver és felhasználói oldali informatikai eszközök, illetve hálózati eszközök üzemeltetését.
- Biztosítja a Szervezet informatikai eszközeinek minél kisebb kieséssel történő üzemeltetését. Felügyeli az informatikai eszközök műszaki karbantartását, javítását a leggazdaságosabb megoldásokat helyezve előtérbe.
- Irányítja az új rendszerszoftverek, alaprendszerek bevezetését. Törekszik arra, hogy az üzleti célkitűzéseket támogató és a folyamatok hatékony működését biztosító, korszerű informatikai rendszerek kerüljenek kialakítása.
- Fokozott figyelmet fordít az informatikai rendszerek bevezetése és továbbfejlesztése során az IBSZ-ben rögzített információbiztonsági előírások teljesülésére. Ennek során együttműködik az IBF-fel.

INFORMÁCIÓBIZTONSÁGI FELELŐS (RÖVIDÍTVE: IBF)

Az Ibtv.-nek megfelelően az elektronikus információs rendszerek biztonságáért felelős személy, az Intézményvezető által kinevezett személy.

FELADATAI:

- Felelős a Szervezetnél előforduló valamennyi, az informatikai rendszerek védelméhez kapcsolódó feladat ellátásáért.
- Gondoskodik a Szervezet informatikai rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.
- Elvégzi vagy irányítja az előző pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.
- Előkészíti és rendszeresen felülvizsgálja a Szervezet Informatikai Biztonsági Szabályzatát.
- Előkészíti és rendszeresen felülvizsgálja a Szervezet informatikai rendszereinek biztonsági osztályba sorolását és a Szervezet biztonsági szintbe történő besorolását.
- Információbiztonsági szempontból véleményezi a Szervezet szabályzatait és szerződéseit, biztosítja a biztonsági követelmények érvényre juttatását.
- Összeállítja az információbiztonsági ismeretek és előírások oktatási anyagát, megszervezi az információbiztonsági képzések lebonyolítását.
- Részt vesz az informatikai rendszerek bevezetése és továbbfejlesztése során a biztonsági rendszer tervezésében, kialakításában, a védelmi eszközök alkalmazására vonatkozó döntés előkészítésben, a biztonságot növelő intézkedések kialakításában.
- Kockázatelemzés végzésével követi az informatikai rendszereket fenyegető veszélyforrások változásait és kezdeményezi a szükséges védelmi intézkedéseket. Javaslatot tesz új védelmi eszközök és technológiák beszerzésére, illetve bevezetésére
- Bejelentés alapján kivizsgálja a biztonsági eseményeket, és javaslatot tesz további intézkedésekre.
- Kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.
- Évente legalább egyszer ellenőrzi az IBSZ előírásainak betartását, és erről beszámol az informatikai vezetőnek és a Szervezet vezetőjének.
- Írásban jelent a Szervezet vezetőjének minden olyan vitás kérdést, melyet az érintett területekkel együttműködve nem tud rendezni, illetve a biztonsági előírások teljesülésének veszélyeztetését észleli és közvetlen intézkedése eredménytelen maradt.
- Az IBSZ súlyos megszegését jelenti az informatikai vezetőnek, aki az előírások ellen vétőkkel szemben fegyelmi felelősségre vonási eljárást kezdeményezhet

JOGAI:

- Jogosult az IBSZ előírásainak betartását bármely érintett szervezeti egységnél ellenőrizni.
- Ellenőrzési tevékenysége során betekintést nyerhet az informatikai rendszerek működésébe és a kapcsolatos dokumentumokba.
- Közvetlenül jogosult bármely érintett szervezeti egység vezetőjének, beosztott munkatársának olyan utasítást adni, mely az IBSZ-ben foglaltak betartását, annak végrehajtását célozza.
- Feladata ellátása során a Szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

ADATVÉDELMI FELELŐS

Az Infotv. előírásainak és a Szervezet hatályos *Adatvédelmi és Adatbiztonsági Szabályzatának* szervezeten belüli betartásáért felelős személy.

Felelőssége nemcsak az informatikai rendszerekben kezelt adatokra vonatkozik, hanem minden adatkezelésre függetlenül annak megjelenési formájától (pl.: papír alapú nyilvántartásokra, szerződésekre, dokumentumokra stb.).

FELADATAI:

- Szorosan együttműködik az IT csoporttal, segíti annak munkáját és iránymutatást nyújt adatkezeléssel összefüggő kérdésekben.
- Ellenőrzi az adatvédelmi előírások betartását.
- Egyéb adatvédelmi feladatait az *Adatvédelmi és Adatbiztonsági Szabályzat* határozza meg.

PORTASZOLGÁLAT

A Szervezet vezetője által a fizikai belépések felügyeletével megbízott munkatárs

FELADATAI:

- Folyamatosan karbantartja a Szervezet épületeibe belépésre jogosultak listáját, kiadja és visszavonja a belépési engedélyeket, illetve az engedélyek igazolására szolgáló belépőkártyákat
- Felügyelet alatt tartja a fizikai belépések folyamatát, kezeli az ezzel kapcsolatos rendellenességeket

BELSŐ RENDSZERGAZDA

Az informatikai rendszerek felett a Szervezet részéről felügyeletet gyakorló személy (aki rendszerint az alaprendszerek esetén rendszergazda munkakörben, alkalmazói rendszerek esetén alkalmazás üzemeltető munkakörben dolgozó munkatársa). Biztonsági szempontból az informatikai rendszerek felhasználó oldali végberendezéseiért is felelős.

FELADATAI:

- Biztosítja a felhasználó oldali informatikai eszközök (számítógépek és tartozékok) működőképességét, fenntartja a folyamatos munkavégzéshez szükséges állapotot.
- Elvégzi az új eszközök IBSZ-ben rögzített információbiztonsági előírásoknak megfelelő biztonsági beállítását, és folyamatosan biztosítja a biztonsági beállítások helyességét és sértetlenségét.
- Az elhasználódott eszközök, adathordozók selejtezése, illetve újra felhasználásra kiadása esetén biztosítja a szükséges adatok mentését és az adathordozók biztonságos törlését, illetve megsemmisítését.
- Fokozott figyelmet fordít arra, hogy a szervereket/egyéb eszközöket kiemelt jogosultságokkal bejelentkezett állapotban ne hagyja felügyelet nélkül magára, a feladata elvégzése után kijelentkezik a rendszerből.

KÜLSŐ RENDSZERGAZDA

Az informatikai rendszerek felett az Üzemeltető részéről felügyeletet gyakorló személy (aki rendszerint az alaprendszerek esetén rendszergazda munkakörben, alkalmazói rendszerek esetén alkalmazás üzemeltető munkakörben dolgozó munkatársa).

FELADATAI:

- Felelős a rábízott informatikai rendszer üzemszerű, folyamatos működéséért. Rendszeresen ellenőrzi a rendszer és elemeinek helyes működését.
- Felügyeli az informatikai rendszer (és környezetének) biztonsági állapotát. Folyamatosan ellenőrzi az informatikai rendszer védelmi eszközeinek megfelelő működését. Felelős a biztonsági kockázatok minimalizálásáért, az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismeréséért és jelentéséért.
- Felelős az informatikai rendszer biztonsági mentéseinek készítéséért, ellenőrzéséért, tárolásáért és a kapcsolódó nyilvántartások vezetéséért.
- Elkészíti, rendszeresen felülvizsgálja és teszteli a Szervezet *Katasztrófa elhárítási tervét*.
- Gondoskodik az informatikai rendszer katasztrófahelyzetben történő újraindíthatóságáról, illetve az ehhez szükséges beállítások, paraméterek rendelkezésre állásáról.
- Az informatikai rendszerre vonatkozóan feltölti és naprakészen tartja az *Informatikai rendszerek nyilvántartását,* a rendszer *Alapkonfigurációját* és az *Rendszerelem leltárt*
- Elvégzi az informatikai rendszer hibáinak felderítését, az ebből adódó szoftvertelepítési, frissítési feladatokat, valamint koordinálja a külső partnerek által végzett javításokat.
- Az informatikai rendszer kialakítása és üzemeltetése során biztosítja az információbiztonsági és adatvédelmi előírások feltételeit és figyelemmel kíséri az előírások betartását. Mindezek tekintetében együttműködik az IBF-fel és az adatvédelmi felelőssel.

- Indokolt esetben az informatikai vezető tájékoztatásával és jóváhagyásával dokumentáltan engedélyezi az előírt üzemeltetéstől eltérő eljárások, konfigurációk alkalmazását.
- Nyomon követi az informatikai rendszer változásait, és ennek megfelelően módosítási javaslatokat dolgoz ki.
- Véleményezi az esetleges fejlesztési igények megvalósíthatóságát, az új védelmi megoldások beépíthetőségét a működő rendszerbe.
- Fogadja az e-mailben és sürgős esetben telefonon érkező felhasználói bejelentéseket és amennyiben szükséges, az egységes kezelés érdekében rögzíti a Helpdesk rendszerben.
- A Helpdesk-en bejelentett biztonsági eseményekről az esemény kivizsgálása céljából értesíti az IBF-t.

ADATGAZDAI TERÜLET VEZETŐJE

Annak a szervezeti egységnek (adatgazdai területnek) a vezetője, amely szervezeti egységhez az informatikai rendszerben tárolt adatok kezelése rendelhető, illetve ahol az adat keletkezik.

FELADATAI:

- Meghatározza az adatok kezelésének célját, és meghozza az adatkezelésre vonatkozó döntéseket (beleértve a felhasznált eszközök megválasztását).

KULCSFELHASZNÁLÓ

Az informatikai rendszerekhez az adatgazdai terület részéről kijelölt, a rendszerben tárolt adatok védelméért, a rendszer funkcionális működéséért felelős felhasználó.

FELADATAI:

- Folyamatosan figyelemmel kíséri a felügyelete alá rendelt informatikai rendszer megfelelő működését. Ha hibás működést tapasztal, erről a Helpdesk-en értesíti az Üzemeltetőt.
- Közreműködik a Szervezet *Üzletmenet folytonossági tervének* elkészítésében, elvégzi a terv rendszeres tesztelését.
- Az informatikai rendszer hibás működése esetén, ha úgy ítéli meg, az *Üzletmenet folytonossági terv* alapján eljárva kezdeményezi a rendszer használatának felfüggesztését, és írásban rögzíti a felfüggesztés okát, a tapasztalt jelenséget. Ezzel egyidejűleg erről értesíti az IT csoportot és szükség szerint az intézkedésre jogosult elöljáróját. Továbbá intézkedik arról, hogy a munkafolyamatok rögzítése a rendszer helyreállításáig papír alapú bizonylatokon történjen.
- Engedélyezi a külső és belső felhasználók különböző szintű hozzáférését az informatikai rendszerhez.
- Felügyeli, karbantartja az informatikai rendszer kódrendszerét. Más rendszerekkel közös, kiemelt kódok esetén egyeztet a kapcsolódó rendszerek kulcsfelhasználóival és a kódfelelőssel.
- Gondoskodik az informatikai rendszerrel dolgozó felhasználók betanításáról, a kezelési és információbiztonsági szabályok megismertetéséről. Ehhez szükség szerint segítséget kérhet az IT csoporttól és az IBF-től.
- Gondoskodik az információbiztonsági és adatvédelmi előírások maradéktalan betartatásáról az adatfeldolgozás során (ez különös figyelmet kíván a személyes adatokat és a Szervezet eredményességét jellemző adatokat kezelő informatikai rendszerek kulcsfelhasználóitól). Együttműködik az IBF-fel és az adatvédelmi felelőssel.
- Összefogja és koordinálja az informatikai rendszerrel kapcsolatban felmerülő fejlesztési, módosítási, javítási igényeket, ezeket képviseli a IT csoport, illetve a rendszer külső fejlesztői felé. Kapcsolatot tart z Üzemeltetővel.
- Vezeti az új vagy módosított informatikai rendszer tesztelését. Felelős azért, hogy a tesztelés úgy történjen, hogy abból legyen tapasztalat minden üzemszerű működtetési körülményre, és lehetőség szerint nem üzemszerű működtetésre is.

MUNKAHELYI VEZETŐ

A Szervezet vezetése és a további vezetők.

FELADATAI:

- Felelős a saját területén a jelen eljárás betartásáért és betartatásáért. Köteles az IBSZ-ben foglaltakat megismerni és azt a munkaterületük beosztott munkatársaival megértetni, a rájuk bízott feladatokat határidőre elvégeztetni, és a végrehajtást folyamatosan ellenőrizni.

FELHASZNÁLÓ

Az informatikai rendszerekkel kapcsolatba kerülő, azt használó munkatársak.

FELADATAI:

- Minden felhasználó köteles megismerni és betartani az IBSZ-ben leírtakat.
- Jelenti a jogszabályokban, szabályzatokban megfogalmazott előírások bárki által történő megszegését a munkahelyi vezetőjének, továbbá az IBSZ megszegését az IBF-nek.
- Köteles jelenteni, ha biztonsági problémát okozó jelenséget (biztonsági eseményt) észlel.
- Figyelemmel kíséri az informatikai rendszerek működését. Ha hibás működést tapasztal, erről azonnal értesíti a rendszer kulcsfelhasználóját és sürgős esetben a Helpdesk-en keresztül közvetlenül a IT csoportot. Rendellenes működés esetén nem szabad az adatfeldolgozást folytatnia.
- Együttműködik az információbiztonságért és informatikai üzemeltetésért felelős személyekkel. Karbantartás előtt szükség esetén segítséget nyújt az üzemeltető munkatársnak a számítógépen tárolt adatok mentéséhez.
- Nem hagyja bejelentkezett állapotban felügyelet nélkül a számítógépét. Ha távozik a számítógéptől vagy befejezi a munkát, kilép az alkalmazói rendszerekből és zárolja, illetve kikapcsolja számítógépet. Ha utolsóként távozik a helyiségből, a Szervezet előírásainak megfelelően zárja a helyiséget.
- A karbantartásokat, javításokat helyben végző külső partnerek szakembereit még átmeneti időre sem hagyhatja felügyelet nélkül.
- Köteles meghatározott időközönként információbiztonsági képzésen részt venni. Csak a képzés eredményes megtörténtét követően dolgozhat az informatikai rendszerekben.
- Szakszerűen kezeli a munkavégzéséhez biztosított informatikai eszközöket (a számítógépet és a hozzá kapcsolt tartozékokat).
- Gondoskodik az informatikai eszközök állagmegóvásáról, a rárakódott szennyeződések eltávolításáról. Óvja nedvességtől, víztől, mágneses és elektromos erőtértől, mechanikai behatásoktól. Szintén óvja a hálózat elemeit (fali hálózati csatlakozók, kábelek).
- Az informatikai eszközök sérülését azonnal jelenti a Helpdesk-en a IT csoportnak.
- Gondoskodik a nevére szólóan kiosztott belépőkártya megfelelő kezeléséről és őrzéséről.
- Köteles az informatikai rendszerekhez hozzáférést biztosító jelszavait titokban tartani. A felhasználó viseli a felelősséget minden műveletért, amely neki felróható mulasztás miatt az adott felhasználóhoz tartozó azonosítóval kerül.

JOGAI:

- A felhasználók jogosultak a rájuk vonatkozó jogszabályok, szabályzatok és a munkájukhoz szükséges információbiztonsági előírások megismeréséhez.
- Jogosultak az informatikai rendszerek technikai problémáiról, tervezett karbantartásokról vagy rendkívüli eseményekről tájékoztatást kapni.
- Jogosultak megtagadni a számítógépes munkát, ha az súlyos törvénysértéshez, vagy bűncselekményhez vezetne.
- Jogosultak a számítógépes munkavégzéssel kapcsolatos sérelmeiknek jogorvoslati kezelésére. Jogorvoslati kérdésekben az informatikai vezető, magasabb szinten a Szervezet vezetője áll rendelkezésre.
- Jogosultak a számítógépes tevékenységük során felmerült problémák, akadályok elhárításához támogatást kapni az IT csoporttól. A segítségnyújtáshoz az igényt a HelpDesk-en kell bejelenteni.

3.1.4.2.1.10. ALAPFELADATOK BIZTOSÍTÁSA

A Szervezet fenntartja a szervezet által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása, vagy hibája ellenére is.

3.1.4.2.1.11. HELYREÁLLÍTÁS

Az alternatív rendszer indításához az alábbi adatbázisokra van szükség:

- ügyféltörzs
- nyilvántartási adatok
- érvényes díjak és kötelezettségek
- szerződés adatok

Ezen adatok kinyerhetőek az éles rendszer mentéseiből, illetve az adatbejelentésekből.

3.1.4.3. A FOLYAMATOS MŰKÖDÉSRE FELKÉSZÍTŐ KÉPZÉS

3.1.4.3.1. AZ ÉRINTETTEK MEGHATÁROZÁSA

A Szervezet az elektronikus információs rendszer folyamatos működésére felkészítő képzést tart a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően.

Az üzletmenet-folytonosság megfelelő szinten tartása, valamint a nem várt események esetén alkalmazandó *Üzletment folytonossági terv* és *Katasztrófa elhárítási terv* megfelelő hatékonysággal történő végrehajtása érdekében a tervek végrehajtásában érintett szereplők részére a szerepkörbe kerülésüket vagy a tervek változását követően felkészítő és évente ismétlő képzéseket kell tartani.

A képzéseken a következő területeket kell legalább érinteni:

- az informatikai rendszerekre ható főbb fenyegetéseket;
- a fenyegetések minimalizálása érdekében megtett kockázatkezelő intézkedéseket;
- a konfigurációkezelési és változáskezelési eljárások megfelelő használatát;
- a mentési eljárásokat;
- a katasztrófa esetén szükséges lépéseket.

A képzés tartalmának összeállítása és a képzés lebonyolítása az IBF feladata.

3.1.4.3.1.1. A KÉPZÉS HATÁRIDEJE

A képzést az új dolgozóknak, munkába állásuk utáni 30 napon belül kell megtartani.

3.1.4.3.1.2. RENDSZERESSÉG

A képzéseket a Szervezet évente szervezi, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik.

3.1.4.8. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI

3.1.4.8.1.1. A MENTÉSI RENDSZER DEFINIÁLÁSA

A Szervezet meghatározott (3.1.1.1.3.14) tartalommal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

A hálózati merevlemezeken található adatok és beállítások rendszeres mentése a rendszergazdák feladata.

A munkaállomásokon található adatok rendszeres mentése a felhasználó feladata.

Az adatok mentése független adattárolóra történik. A kiemelten fontos adatok az Intézményvezető egyedi döntése alapján optikai adathordozóra is menthetők, de ebben az esetben legalább 2 másolatot kell készíteni.

Ha az informatikai rendszer mentéseit nem közvetlenül maga a rendszergazda kezeli, hanem a központi mentőrendszer segítségével került megvalósításra, akkor a központi mentőrendszer rendszergazdájával egyeztetve a rendszergazda felelőssége a mentendő adatok körének, a mentések gyakoriságának és megőrzési idejének meghatározása, és a központi mentőrendszer rendszergazdája gondoskodik a mentések kezelésének többi feladatáról.

A központi mentőrendszer a mentés céljára szolgáló szerverből, mentő szoftverből és szalagos egységekből áll, és a mentések automatikus időzítéssel éjszakai és hétvégi időszakban, szalagos adathordozókra készülnek. Fizikailag a mentő szerver az Üzemeltető központi szervertermében találhatók.

A mentések során olyan eljárást kell alkalmazni, amely egyértelműen biztosítja, hogy a mentés adathordozókra az adatok sértetlenül és visszaolvashatóan felírásra kerüljenek.

A mentések visszaállításához biztosítani kell a háttérkörnyezetet, annak érdekében, hogy a mentett adatok és szoftverek esetleges adattároló hiba, az informatikai rendszerek összeomlása vagy megsemmisülése esetén visszaállíthatóak legyenek.

3.1.4.8.1.2. A MENTÉSEK GYAKORISÁGA

A Szervezet meghatározott (3.1.1.1.3.14) gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

Az egyes informatikai rendszerekre vonatkozóan a rendszergazda az adatok fontosságát és változási ütemét, valamint a mentés elkészítéséhez szükséges időt figyelembe véve előírhat a napi rendszerességtől eltérő, heti vagy havi gyakoriságú mentéseket is.

A MENTÉSI RENDSZER DOKUMENTÁLÁSA

A mentések rendszerét a *Katasztrófa elhárítási terv* mellékleteként kell dokumentálni.

A mentési rendszer dokumentációjának célja, hogy

- a mentések visszaállításához információval szolgáljon a rendelkezésre álló mentésekre vonatkozóan;
- biztosítsa a mentőrendszer személyektől független üzemeltetését;
- a mentőrendszer összeomlása esetén újra lehessen építeni a rendszert.

A dokumentációnak tartalmaznia kell:

- a mentéseket megvalósító mentési feladatokat (mentés job-okat);

- a mentés módját (milyen eszközzel, milyen adathordozóra történik a mentés);
- a mentés típusát (teljes mentés, vagy csak az utolsó teljes mentés óta történt változásokat tartalmazó különbségi mentés);
- a mentés tartalmát (a mentendő adatok helyét);
- a mentések gyakoriságát (napi, heti, havi), indulási idejét;
- a mentések megőrzési idejét;
- a mentési feladat által mentett adatmennyiséget és a mentés időtartamát (a szükséges adathordozók mennyiségének meghatározásához és a különböző mentési feladatok időzítésének összehangolásához);
- a mentési feladatokat megelőző feladatokat (pl. az adatbáziskezelő szoftver által a szerver háttértárjára végzett mentéseket, amelyet a mentési feladat ír ki a mentés adathordozókra) és ezek időzítését;

ALAPRENDSZEREK MENTÉSE

Az alkalmazói szoftverek környezetének, az alap informatikai szolgáltatásokat megvalósító rendszereknek (alaprendszereknek) a biztonsági mentéséről a kijelölt külső rendszergazdának kell gondoskodnia.

A mentésnek ki kell terjednie az alábbi aktív hálózati eszközökre és szerver funkciókra:

- aktív hálózati eszközök (switch-ek, router-ek és vezeték nélküli hozzáférési pontok) konfigurációs beállításai;
- tűzfalak szabálylistája;
- központi címtár adatbázisa;
- DNS szerverek adatbázisa;
- központi levelezés;
- központi weboldalak.

3.1.4.8.1.3. DOKUMENTÁCIÓK MENTÉSE

A Szervezet minden változásakor elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal. A korábbi dokumentációk, verzió szám megjelöléssel tárolandók.

3.1.4.8.1.4. A MENTÉSEK TÁROLÁSÁNAK ALAPELVEI

A Szervezet megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen. A mentések biztonsági szintjei azonosak az éles rendszer biztonsági szintjeivel.

SZOFTVEREK MENTÉSE

Az informatikai rendszer telepítésekor a rendszergazdának mentést kell végeznie a rendszerről, amit minden konfigurációváltoztatáskor és a változáskezelés hatálya alá eső, a rendszer működését befolyásoló beavatkozáskor ismételten el kell végeznie.

- Technikailag ezeket a mentéseket az adatok mentésével együtt kell végezni.

ESEMÉNYNAPLÓK MENTÉSE

A biztonsági események utólagos kivizsgálása érdekében gondoskodni kell az informatikai rendszer eseménynaplóinak mentéséről.

- Technikailag ezeket a mentéseket az adatok mentésével együtt kell végezni.

KAPCSOLÓDÓ DOKUMENTÁCIÓK MENTÉSE

Az informatikai rendszerhez kapcsolódó dokumentációk, szabályzatok, eljárásrendek mentéséről is gondoskodni kell.

- A kapcsolódó dokumentációk mentését minden egyes változtatás esetén el kell végezni.
- Technikailag ezeket a mentéseket az adatok mentésével együtt kell végezni.

ARCHIVÁLÁS

Az adattárolók helytakarékos használatához szükség lehet a ritkán használt vagy használaton kívüli, meghaladottá vált, de nem selejtezhető adatok, szoftverek archiválására, azaz hosszú távú megőrzés céljából adathordozóra írására és törlésére az elsődleges adattárolóról.

A Szervezet archiválást végezhet a következő adatokra vonatkozóan:

- informatikai rendszerek bevezetése, migrációja kapcsán keletkezett adatok;
- szoftverfrissítések vagy egyéb változásokkal kapcsolatos telepítő állományok, funkcionális mentések;
- kilépett munkatársak mentett felhasználói adatai;
- folyamatosan keletkező naplófájlok, felhasználói lekérdezések;
- egyéb felhasználói igények alapján meghatározott adatok.

Az archiválást a felhasználói oldallal egyeztetve lehet elvégezni és a HelpDesk-en kell dokumentálni.

Az informatikai rendszerrel kapcsolatos archiválási igényeket a rendszer kulcsfelhasználójának a HelpDesk-en kell bejelentenie.

MENTÉSEK ROTÁCIÓS RENDJE

A mentések készítésére a Szervezet a következő rotációs rendet követi:

- a hétköznapokon napi mentést készít (rendszerint csak az utolsó teljes mentés óta történt változásokat tartalmazó, ún. különbségi mentést);
- a hétvégén készülnek a heti mentések (teljes mentések);
- az adott hónapot követő első heti mentést havi mentésként kezeli;
- minden havi mentésből az utolsót éves mentésként kezeli;
- a heti mentésekkel együtt igény szerint készülhetnek archív mentések;
- a napi, heti, havi, éves és archív mentések különböző megőrzési idővel elkülönített adathordozókra történnek.

ADATOK HOSSZÚ TÁVÚ MEGŐRZÉSE

A Szervezetre vonatkozó jogszabályokban előírtak alapján a pénzügyi-számviteli rendszer adatait (pl. számlázási adatokat) 8 évig kell megőrizni; a munkaügyi-, bér- és társadalombiztosítási adatok pedig egyáltalán nem selejtezhetőek.

A jogszabályokban előírtak és a Szervezet elvárásai alapján a megőrzési idők teljesülése érdekében a következő előírásokat kell alkalmazni:

- a napi mentések megőrzési ideje minimum 1 hét;
- a heti mentések megőrzési ideje minimum 1 hónap;
- a havi mentések megőrzési ideje az eseménynaplókra vonatkozóan 1 év, egyéb adatok esetén minimum 3 hónap (eltérő megőrzési idők esetén az eseménynaplók mentésére elkülönített adathordozókat kell használni);
- az éves és az archív mentéseket 10 évig kell megőrizni;
- a számlázási adatok az éles számlázási rendszerből 10 évig nem törölhetőek;
- a munkaügyi-, bér- és társadalombiztosítási adatok nem törölhetőek a rendszerből.

ADATHORDOZÓK NYILVÁNTARTÁSA

Az archív állományokat tartalmazó adathordozókat, nyilván kell tartani, az alábbi adatok megjelölésével:

- Milyen adat található rajta
- Mentés ideje
- Meddig őrizhető
- Személyes adatok jelenléte
- Tárolási helye
- Sorszáma

A mentések adathordozóit biztonságos környezetben, elzárva kell őrizni. A napi mentések kivételével a többi mentés adathordozóit a szerverteremtől eltérő helyszínen (lehetőség szerint eltérő telephelyen, de legalább eltérő épületben) kell tárolni.

Az adathordozókat egyedi azonosítóval kell ellátni, az *Adathordozók nyilvántartása* vezetésével nyilván kell tartani és visszakereshető formában kell tárolni.

A központi mentőrendszerre vonatkozóan az elvégzett mentési feladatok és a mentés adathordozók tartalmának tételes nyilvántartása elektronikus formában, a mentést végző szoftver által történik. A szoftver belső adatbázisa tartalmazza továbbá a mentési feladatok időzítését, beállításait is. Mindezek miatt a mentőszoftver adatbázisát is rendszeresen menteni kell a többi informatikai rendszer mentésével együtt.

Az elhasználódott vagy meghibásodott adathordozók cseréjének szükségességét a mentőszoftver jelzi.

3.1.4.9. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER HELYREÁLLÍTÁSA ÉS ÚJRAINDÍTÁSA

3.1.4.9.1. A HELYREÁLLÍTÁS

A Szervezet az üzletmenet folytonossági előírásoknak megfelelően gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást, vagy hibát követően.

Az informatikai erőforrásokat érintő katasztrófa esetén az *Üzletmenet-folytonossági tervben* és a *Katasztrófa Elhárítási tervben* szereplő lépések végrehajtásával kell visszaállítani a normál (vagy a rendszer teljes visszaállításig a csökkentett funkcionalitású) működést.

A kiemelten fontos eszközökre vonatkozóan külső partnerekkel kell szerződést kötni, hogy az eszközöket megadott időn belül kijavítsák, vagy helyettesítésükről gondoskodjanak. A kiemelt fontosságú eszközök meghatározása és a szerződés megkötése az informatikai vezető felelőssége.

A rendszergazdának gondoskodnia kell az informatikai rendszerek helyreállításához szükséges mentések meglétéről, elérhetőségéről.

A szerverteremben működő informatikai eszközök vészleállításának és újraindításának folyamatát leíró dokumentumot (Szerverterem vészleállítása és újraindítása) a rendszergazda állítja össze, és az informatikai vezető hagyja jóvá. A dokumentum egy példányát a szerverteremben kell tárolni.

A portaszolgálat tudomására kell hozni a tervekben szereplő azon munkatársak a névsorát, akik a helyreállítás kapcsán akár munkaidőn kívül, a lezárt épületekbe is bejuthatnak.

VISSZAÁLLÍTÁS TESZTELÉSE

Évente legalább egyszer meg kell győződni a mentések használhatóságáról az adatok visszaállításával. Az ellenőrzés történhet felhasználói igény alapján végzett visszaállítással vagy ennek hiányában az éves mentésből történő visszaállítással. Az ellenőrzést és az eredményét a HelpDesk rendszerben kell dokumentálni.

3.1.5 A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

3.1.5.1.1. ESEMÉNYKEZELÉSI ELJÁRÁS

Az informatikai rendszerekben előforduló biztonsági események hatékony, gyors kezelése érdekében, biztonsági események gyanúja esetén a következő Biztonsági eseménykezelési eljárásrendet kell alkalmazni.

A felhasználó köteles az általa tapasztalt rendellenes eseményeket az üzemeltetővel azonnal közölni, szóbeli közlés esetén legkésőbb a következő munkanapon írásban is megerősíteni. Köteles a teljes körű igazságot elmondani az előzményekről, még akkor is, ha e szabályzat megszegése az előzmények része.

Ha a felhasználónak gyanúja támad arra, hogy a jelszavát más személy is megismerte vagy személyazonosító eszközét más megszerezte vagy lemásolta, a felhasználó köteles azonnal jelezni ezt az üzemeltető felé, továbbá amennyiben a lehetőségei adottak, köteles a jelszavát azonnal megváltoztatni, személyazonosító eszközét letiltatni a megfelelő szolgáltatónál.

Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett eszközt le kell választani a hálózatról, illetve szükség esetén ki kell kapcsolni.

Vírustámadás esetén fokozottan figyelni kell a cserélhető adathordozókra is. A fertőzött számítógépben használt adathordozók kizárólag a vírusellenőrzést követően használhatók más számítógépeken.

A Rendszergazda gondoskodik arról, hogy a többféle módon (web-es felületen, e-mailben és sürgős esetben telefonon) bejelentett biztonsági események minden esetben a „Biztonsági esemény” kategóriába kerüljenek. A HelpDesk rendszer beállításával biztosítani kell, hogy ebbe a kategóriába tartozó bejelentésekről az IBF azonnali e-mail értesítést kapjon. A Rendszergazda ezen kívül telefonon vagy személyesen is jelenti az eseményt az IBF-nek.

3.1.5.1.2. EGYEZTETÉS

A Szervezet egyezteti az eseménykezelési eljárásokat az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel.

3.1.5.1.3. KÖVETKEZTETÉSEK

A Szervezet az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe és tesztelésbe.

3.1.5.4. A BIZTONSÁGI ESEMÉNYEK FIGYELÉSE

3.1.5.4.1. NYOMON KÖVETÉS

Az eseményekről értesített feladata a szükséges intézkedések meghozatala, a teljes elhárítási folyamat dokumentálása.

Az incidensekről készült feljegyzéseket az IT biztonságért felelős vezető rendszeresen áttekinti, szükség esetén további helyesbítő, megelőző intézkedésekre tesz javaslatot.

3.1.5.6. A BIZTONSÁGI ESEMÉNYEK JELENTÉSE

3.1.5.6.1.1. JELENTÉSI KÖTELEZETTSÉG

Minden munkatárs feladata, hogy az információbiztonsági incidenseket, észlelt gyengeségeket jelentse közvetlen felettesének, eredménytelenség esetén az IT Biztonságért felelős vezetőnek.

Biztonsági eseménynek nevezzük az informatikai rendszerek működésében beállt olyan kedvezőtlen változást, amelynek hatására az informatikai rendszer vagy a benne kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása sérült vagy sérülhet.

A jellemző biztonsági események a következők:

- szoftver vagy hardver hibás működése;
- nem ellenőrzött rendszerbeli változások;
- a bizalmasság és/vagy sértetlenség sérülése;
- informatikai eszközök elvesztése;
- vírusok és egyéb kártevők általi fertőzés;
- túlterheléses támadások (szolgáltatás megtagadó, DoS támadások);
- az informatikai rendszerrel való visszaélés;
- a szabályzatoknak vagy irányelveknek való nem megfelelés;
- a fizikai biztonsági rendelkezések megsértése;
- a hozzáférési előírások megsértése;
- emberi hibák.

3.1.5.6.1.2. HATÓSÁGI BEJELENTÉS

A Szervezet a jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek.

3.1.5.7. SEGÍTSÉGNYÚJTÁS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉHEZ

Az IBF feladata, hogy tájékoztatást és segítséget nyújtson az informatikai rendszerek felhasználóinak a biztonsági események észlelése, kezelése és jelentése érdekében.

3.1.5.7.1. SUPPORT

A Szervezet belső tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez.

3.1.5.8. BIZTONSÁGI ESEMÉNYKEZELÉSI TERV

3.1.5.8.1.1. A BIZTONSÁGI ESEMÉNYKEZELÉSI TERV TARTALMA

Az informatikai biztonsági események és gyengeségek követése szabályozott kezelése érdekében a következő szabályokat kell rögzíteni:

- Az informatikai biztonsági eseménynek és gyengeségek bejelentésének és eszkalációjának szabályai
- Az informatikai biztonsági eseménynek és gyengeségek kezelésére vonatkozó szabályok

A biztonsági események kezelésére felkészülve a Szervezetnek *Biztonsági eseménykezelési tervet* kell kidolgoznia, amely iránymutatást ad az események kezelési módjaira.

A tervnek tartalmaznia kell:

- a bejelentés-köteles biztonsági események meghatározását (tipikus példákkal az egyes esemény fajtákra);
- a biztonsági események súlyosság szerint kategorizálásának módját;
- az egyes a biztonsági események Szervezethez illeszkedő kezelésének módját (ahol előre meghatározható konkrét eseménykezelési lépéseket megadva, egyébként átfogó megközelítést nyújtva);
- a biztonsági eseményeket kezelő szerepköröket, ezek felelősségét, feladatait;
- a biztonsági események belső mérésének, kiértékelésének módját (amely mérési eredményeket, tapasztalatokat fel kell használni a kockázatelemzésnél, az eseménykezelési terv felülvizsgálatánál és be kell építeni az információbiztonsági képzésekbe);
- azon erőforrásoknak és vezetői támogatásnak a meghatározását, amelyek szükségesek a biztonsági eseménykezelési lehetőségek fenntartásához, illetve bővítéséhez, hatékonyabbá tételéhez.

A terv elkészítéséért és karbantartásáért – a rendszergazdákkal egyeztetve – az IBF a felelős. A terv jóváhagyása az informatikai vezető feladata.

A *Biztonsági eseménykezelési terv* bizalmas minősítésű dokumentum, amelyeket az eseménykezelésben érintett személyek, szervezeti egységek számára kell kihirdetni, akik illetékteleneknek nem adhatják tovább. A terv megismerésére (és tárolására) jogosult szereplők feladata gondoskodni arról, hogy a terv jogosulatlanok számára ne legyen megismerhető, módosítható.

A tervet frissíteni kell, és évente felül kell vizsgálni, figyelembe véve az informatikai rendszerek és a Szervezet változásait vagy a terv megvalósítása, végrehajtása során felmerülő problémákat.

A terv változásairól tájékoztatni kell a tervekben érintett szereplőket.

3.1.5.8.1.1.1. KEZELÉSI MÓDOK

A Szervezet a biztonsági eseményeit súlyosságuk szerint priorizálja, és ennek megfelelően kezeli.

3.1.5.8.1.1.2. LEHETŐSÉGEK

A Szervezet a biztonsági események kezeléséhez szükség szerint munkacsoportokat jelöl ki, ezek tagjai az üzletmenet folytonossági előírásokban érintett szerepkörökből, és személyekből kerülhetnek ki.

A biztonságos és megbízható üzemeltetés érdekében védelmi intézkedéseket szükséges bevezetni. Ennek megfelelően rögzíteni kell a következő szabályokat:

- A rendszerek üzemeltetésére vonatkozó szabályok
- Külső szolgáltatók nyújtotta szolgáltatások igénybevételére vonatkozó szabályok
- Rendszerek tervezésre és bevezetésre vonatkozó szabályok
- A rosszindulatú szoftverek negatív hatásainak megelőzésére, ill. kezelésre vonatkozó szabályok
- A biztonsági mentésre vonatkozó szabályok
- A hálózati működésre vonatkozó szabályok
- Az adathordozók kezelésre vonatkozó szabályok
- Az biztonságos adattovábbításra vonatkozó szabályok
- Az e-kereskedelemre vonatkozó szabályok
- A naplózásokra vonatkozó szabályok

3.1.5.8.1.1.3. LEHETŐSÉGEK ILLESZKEDÉSE

A Szervezet biztonsági eseménykezelésének úgy kell megvalósulnia, hogy a beruházási igények a gazdasági, a logikai igények pedig az informatikai ellenőrzésre jogosultak hatókörébe kerüljenek. Amennyiben humánerőforrás bevonását igényli a feladat, akkor a személyügyi osztályt is be kell vonni az eseménykezelési folyamatokba.

3.1.5.8.1.1.4. EGYEDI IGÉNYEK

Amennyiben a biztonsági események kapcsán felmerül az informatika szervezeti felépítésével és funkcióival kapcsolatos egyedi igény, azt Szervezet lehetőségeihez kezeli, kielégíti.

3.1.5.8.1.1.5. JELENTÉSI KÖTELEZETTSÉG

Minden esemény jelenteni kell, ami a rendszerek és mentések (archívumok) sértetlenségét, bizalmasságát, és rendelkezésre állását érinti.

HARDVERES HIBABEJELENTÉS

A felhasználók az észlelt hibákat azonnal kötelesek az üzemeltető felé a HelpDesk rendszerben, vagy telefonon jelezni.

A hibabejelentésnek tartalmaznia kell az alábbiakat:

- Esemény megnevezése (hiba leírása)
- A hibával érintett periféria pontos megnevezése
- A hiba ideje
- A hiba felfedezésekor megnyitott állományok, adatbázisok pontos megnevezése
- Az esemény kapcsán közvetve érintett felhasználók felsorolása, behatárolása

3.1.5.8.1.1.6. KIÉRTÉKELÉS

A biztonsági események kiértékelésének, kategorizálásának (súlyosság, stb.) kritériumrendszere:

Prioritás:

- Alapszolgáltatás közvetlen érintettsége (1)
- Alapszolgáltatás közvetett érintettsége (2)
- Egyéb szolgáltatás közvetlen érintettsége (3)
- Egyén szolgáltatás közvetett érintettsége (4)

Súlyosság:

- Működést kizáró ok, vagy állapot (Magas (1))
- Működést akadályozó ok, vagy állapot (Közepes (2))
- Működést zavaró ok, vagy állapot (Alacsony (3))

3.1.5.8.1.1.7. MÉRŐSZÁMOK

A biztonsági események mérőszámát a prioritási és a súlyossági értékék szorzatából kell meghatározni. A legalacsonyabb mérőszámú hiba elhárításával kell kezdeni a folyamatot, azonosság esetén a prioritás a meghatározó.

3.1.5.8.1.1.8. ERŐFORRÁSOK

A Szervezet meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

3.1.5.8.1.2. KIHIRDETÉS

A biztonsági eseménykezelési tervet a Szervezet a biztonsági szabályzattal együtt hirdeti ki, annak elválaszthatatlan részeként.

3.1.5.8.1.3. FELÜLVIZSGÁLAT

A biztonsági eseménykezelési tervet évente szükséges felülvizsgálni, és a tervben szereplő adatok oly mértékű változása esetén, ami ezt indokolttá teszi.

3.1.5.8.1.4. FRISSÍTÉS

Az eseménykezelési terv haladéktalan frissítése akkor esedékes, ha a tervben foglaltak végrehajtása elháríthatatlan akadályokba ütközik.

3.1.5.8.1.5. VÁLTOZÁSKÖVETÉS

A Szervezet a biztonsági eseménykezelési terv változásait a 3.1.5.8.1.2. pont szerint ismerteti.

3.1.5.8.1.6. BIZALMASSÁG

A Szervezetnek gondoskodni kell arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.5.9. KÉPZÉS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉRE

3.1.5.9.1.1. A KÉPZÉSEK SZERVEZÉSE

A Szervezet biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban, a képzés az éves képzési terv elválaszthatatlan eleme.

3.1.5.9.1.2. A KÉPZÉSEK RENDSZERESSÉGE

A képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, 30 napon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, egyéb esetekben évente kell megtartani.

3.1.6.1. SZEMÉLYBIZTONSÁGI ELJÁRÁSREND

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed a Szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki a Szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges vagy feltételezhető kapcsolatba kerülő személy nem a Szervezet alkalmazottja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

A Szervezet minden alkalmazottjának titoktartási nyilatkozatot kell aláírnia, melyben nyilatkozik arról, hogy a munkája, tevékenysége során tudomására jutott, a Szervezet számára értéket jelentő információt sem jogviszonya fennállása idején, sem annak megszűnése után nem hozza harmadik fél tudomására.

A titoktartási nyilatkozat a munkaszerződés részét kell, hogy képezze, amelyről a Munkaügyi csoport vezetőjének kell gondoskodnia.

3.1.6.2. MUNKAKÖRÖK, FELADATOK BIZTONSÁGI SZEMPONTÚ BESOROLÁSA

3.1.6.2.1.1. BESOROLÁSOK (WORKTABLE)

A Szervezet minden munkakört, kapcsolódó feladatot biztonsági szempontból besorol, a besorolás 4 szintre tagozódik, melyek szorosan kapcsolódnak a szervezeti ábrához.

- Felhasználó (Alacsony biztonsági elvárások)
- Középvezető (Közepes biztonsági elvárások)
- Felső vezető (Magas biztonsági elvárások)
- Rendszergazda, fejlesztő (Kiemelt biztonsági elvárások)

3.1.6.2.1.2. NEMZETBIZTONSÁGI BESOROLÁS

A Szervezet bármely munkaviszony keletkeztetésekor felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat. Jelenleg nem található a szervezeti ábrán ilyen szintű besorolás.

3.1.6.2.1.3. FELÜLVIZSGÁLAT

A Szervezet évente felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

3.1.6.3 A SZEMÉLYEK ELLENŐRZÉSE

3.1.6.3.1.1. ELŐZETES ELLENŐRZÉS

A Szervezet az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy a 3.1.6.2.1.1. és 3.1.6.2.1.2. pontok szerinti besorolásnak megfelelő feltételekkel rendelkezik-e.

3.1.6.3.1.2. NEMZETBIZTONSÁGI ELLENŐRZÉS KEZDEMÉNYEZÉSE

Amennyiben a Szervezet a 3.1.6.2.1.2. szerinti munkaköröket betöltő vagy feladatokat ellátó személyek tekintetében megállapítja, vagy észleli az ellenőrzés szükségességét, abban az esetben kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzés végrehajtását.

3.1.6.3.1.3. FELÜLVIZSGÁLAT

A Szervezet folyamatosan ellenőrzi a 3.1.6.3.1. pont szerinti feltételek fennállását.

3.1.6.4 ELJÁRÁS A JOGVISZONY MEGSZŰNÉSEKOR

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges.

3.1.6.4.1.1. Hozzáférések megszüntetése

A jogosultságok megszüntetésének normál folyamata, hogy a kilépő alkalmazottakról a Munkaügyi csoport a HelpDesk-en keresztül értesíti a belső rendszergazdát, aki megszünteti az alkalmazottak jogosultságait.

A hozzáférési jogosultságok megszüntetésével egyidejűleg az elektronikus belépőkártyák jogosultságát is meg kell szüntetni, függetlenül attól, hogy a belépőkártya visszaadásra került-e, vagy sem.

A jogosultságok megszüntetéséért a rendszergazda a felelős.

Hozzáférési jogok visszavonása feladatkör vagy munkakör változás esetén:

A munkavállaló feladatkörének vagy munkakörének változás esetén a munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. Ez esetben is - az új jogosultság igényléséhez hasonló módon – a Hozzáférési jogosultság adatlapot kell kitölteni. Az adatlapon jelölni kell, hogy mely jogosultságokat kell megszüntetni. A jogosultságok részleges visszavonásának eljárásrendje egyéb tekintetben megegyezik az új jogosultsági igény eljárásendjével.

A munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. Amennyiben a hozzáférési jogok részleges visszavonására van szükség, abban az esetben a hozzáférési jog módosítása eljárásrend szerint kell eljárni.

Hozzáférési jogok visszavonása rendes felmondás esetén:

Ha a Szervezet alkalmazottjának munkaviszonya, „rendes” felmondás keretein belül megszűnik, erről a tényről a közvetlen felettesének, illetve a felmondást aláíró vezetőnek haladéktalanul tájékoztatást kell nyújtania az IT csoportnak. Az IT csoport a jelzett időponttal gondoskodik a felhasználó összes rendszerhozzáférésének adott időpontban történő megszüntetéséről vagy letiltásáról, illetve ezek kezdeményezéséről. Az eljárás megtörténtéről az IT csoport tájékoztatja a munkaügyi szervezeti egységet. A munkaviszonyt lezáró dokumentumok között szerepeltetni kell a jogosultságok megszűnéséről szóló tájékoztatást, ebben integráltan egy figyelmeztetést a jogosulatlan belépés, vagy annak kísérletének jogi következményeiről.

Hozzáférési jogok visszavonása rendkívüli felmondás esetén:

Amennyiben a munkavállaló munkaviszonya „rendkívüli” felmondással kerül megszüntetésre, akkor jogosultságainak megszüntetéséről haladéktalanul gondoskodni kell.

Ennek érdekében a felmondást aláíró vezetőnek haladéktalanul tájékoztatnia kell az IT csoportot. Az IT csoport tájékoztatásáért egyetemlegesen felel a felmondást szignáló személy és a munkaügyi ügyintéző. Az IT csoportnak haladéktalanul gondoskodnia kell az illetéktelen hozzáférés megakadályozásáról. A munkavállalónak azonnal írásos tájékoztatást kell kapnia jogosultságai megszűnéséről, és a belépési kísérletek következményeiről.

3.1.6.4.1.2. HITELESÍTŐ ESZKÖZÖK ÉRVÉNYTELENÍTÉSE

A Szervezet a munkaviszony, vagy a szerződéses jogviszony megszűnésekor, érvényteleníti vagy visszaveszi a személy egyéni hitelesítő eszközeit. A visszavétel tényét a munkaviszonyt lezáró dokumentumok között szerepeltetni kell.

3.1.6.4.1.3. TÁJÉKOZTATÁS

A Szervezet tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről (Titoktartás, stb..) A tájékoztatás módja a 3.1.6.4.1.1. pontban szereplő módon történik.

3.1.6.4.1.4. ESZKÖZÖK VISSZAVÉTELE

A Szervezet visszaveszi az elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt. A visszavétel tényét a munkaviszonyt lezáró dokumentumok között szerepeltetni kell.

A vagyontárgyakat a munkahelyi vezetőnek kell átadni, akinek a HelpDesk-en kell igényelnie az átvett informatikai eszközök ellenőrzését és az eszközön lévő felhasználói adatok mentését.

A HelpDesk bejelentés alapján az üzemeltető munkatársnak ellenőriznie kell, hogy az *Üzembe helyezési jegyzőkönyvben* rögzített hardver és szoftver specifikációval adják-e vissza az informatikai eszközöket.

3.1.6.4.1.5. FOLYTONOSSÁG

A Szervezet megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.

A felhasználó személyesen használt dokumentumait, e-mail-jeit le kell menteni az általa használt informatikai eszközökről és a központi tárhelyről, ezzel megelőzve a felhasználó ezekkel kapcsolatos, esetleges információbiztonsági szabályokat sértő magatartását.

A kilépő alkalmazott munkahelyi vezetője rendelkezik arról, hogy a mentett felhasználói adatokhoz a továbbiakban ki férhet hozzá, illetve archiválni, törölni kell-e az adatokat.

Amennyiben a munkahelyi vezető másként nem rendelkezik a mentett felhasználói adatok három hónap után archiválhatók és törölhetők a központi tárhelyről. Az archivált adatokat a jogszabályi és szervezeti előírásoknak megfelelően kell megőrizni és tárolni.

A központi tárhelyen lévő dokumentumok és e-mail-ek mentésére a hozzáférési jogosultságok megszüntetését követően kerül sor, ennek végrehajtásáért a rendszergazda a felelős. A felhasználó informatikai eszközein lévő adatok mentése a munkahelyi vezető bejelentése alapján történik, és a mentést az informatikai munkatárs végzi.

FELADATOK ÁTADÁSA

A kilépő alkalmazott munkahelyi vezetőjének feladata, hogy az alkalmazott informatikai rendszerekkel, vagy azok biztonságával kapcsolatos esetleges feladatainak ellátásáról a munkaviszony megszűnését megelőzően gondoskodjon.

3.1.6.4.1.6. ÉRTESÍTÉS

A Szervezet az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

3.1.6.4.1.7. TITOKTARTÁS

A Szervezet a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik.

Tájékoztatni kell a munkavállalót, hogy a Szervezet informatikai rendszereinek használata során a tudomására jutott minden információ bizalmas adatnak minősül, azok illetéktelen, harmadik fél részére történő továbbadása büntetőjogi, illetve polgári jogi következményeket von maga után és a munkavállaló titoktartási kötelezettsége a munkaviszonya megszűnése után is fennáll.

A munkavállaló tájékoztatásáért a Munkaügyi csoport a felelős.

3.1.6.4.1.8. JOGSÉRTÉSEK MEGELŐZÉSE

A Szervezet a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását minden eszközzel megelőzi.

3.1.6.5 AZ ÁTHELYEZÉSEK, ÁTIRÁNYÍTÁSOK ÉS KIRENDELÉSEK KEZELÉSE

3.1.6.5.1.1. ELŐZETES ELLENŐRZÉS

A Szervezet szükség esetén elvégzi a 3.1.6.3. pontban foglalt, a személyek ellenőrzésére vonatkozó eljárást.

3.1.6.5.1.2. ENGEDÉLYEZÉSI ELJÁRÁS

A Szervezet logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt elektronikus információs rendszerhez, figyelembe véve a szükségesség elvét.

3.1.6.5.1.3. FELÜLVIZSGÁLAT

A Szervezet szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését.

3.1.6.5.1.4. TÁJÉKOZTATÁS

A Szervezet az általa meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

3.1.6.6. AZ SZERVEZETTEL SZERZŐDÉSES JOGVISZONYBAN ÁLLÓ (KÜLSŐ) SZERVEZETRE VONATKOZÓ KÖVETELMÉNYEK

3.1.6.6.1.1. FELELŐSSÉGEK, FELADATOK MEGHATÁROZÁSA

A Szervezet a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is.

Bármely informatikához kapcsolódó szolgáltatást nyújtó szolgáltató, ill. alvállalkozó, valamint más együttműködő partnerrel való együttműködés megkezdése előtt a szerződést előkészítő munkatárs az informatikai biztonságért felelős vezető bevonásával megvizsgálja a felmerülő informatikai biztonsági kockázatokat, hozzáférési igényeket, és a szükséges kontrollokat beépíti a partnerrel kötött szerződésbe, kapcsolódó megállapodásba. Szolgáltató, ill. alvállalkozó bevonása miatt fellépő új kockázat felmerülésekor a kockázatot az informatikai biztonságért felelős vezető a kockázat-felmérési eljárások során kezeli.

A külső partnerek képviselőivel a mindenkor hatályos IBSZ vonatkozó részeit a feladatnak megfelelő mértékben ismertetni kell. A betekintés mélységének meghatározása az IT üzemeltetésért felelős munkatárs (rendszergazda) felelőssége. A szerződéskötés és az együttműködés során biztosítani kell, hogy a külső partner (fejlesztő cég) az általa telepített, fejlesztett informatikai rendszert úgy konfigurálja, hogy annak minden eleme és egésze eleget tegyen az IBSZ-ben előírtaknak.

Az IT vagyontárgyak védelmének megfelelő szintű védelme érdekében nyilvántartásba kell venni és vagyongazdákhoz kell rendelni, továbbá osztályozni szükséges az összes materiális és immateriális vagyontárgyat. A Szervezet rendszereinek informatikai vagyonát leltárlisták tartalmazzák. Ezek alapként szolgálnak a kockázatelemzéshez és a védelmi intézkedések meghatározásához.

A Szervezet adatvagyona informatikai rendszerben van tárolva. Annak érdekében, hogy a különböző informatikai rendszerének sajátosságaiból adódó eltérő védelmi igények érvényre juthassanak, az összetett követelményrendszer egységesen kezelhető legyen, szükség van arra, hogy az informatikai rendszerek eltérő kockázati (belső) besorolásba kerüljenek.

A már meglévő rendszerek cseréje, megújítása esetén meg kell vizsgálni, és szükség esetén az aktuális kockázatoknak megfelelően módosítani kell a belső besorolást. Új rendszerek bevezetésénél el kell végezni a rendszerek besorolását.

3.1.6.6.1.2. KÖVETELMÉNYEK

A Szervezet szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg az itt meghatározott személybiztonsági követelményeknek.

3.1.6.6.1.3. DOKUMENTÁCIÓS KÖVETELMÉNYEK

A Szervezet a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket.

3.1.6.6.1.4. TÁJÉKOZTATÁSI KÖTELEZETTSÉG

a Szervezet előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést a Szervezetnek, és hozza meg a szükséges intézkedéseket.

3.1.6.6.1.5. ELLENŐRZÉS

A Szervezet folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

3.1.6.7. FEGYELMI INTÉZKEDÉSEK

Az IBSZ bárki által történő megszegését az észlelő haladéktalanul köteles jelenteni az IBF-nek.

A Szervezet a felhasználók részéről szándékos károkozásnak tekinti az alábbi tevékenységeket:

- behatolást az informatikai rendszerek környezetébe;
- illetéktelen hozzáférést az adatokhoz, eszközökhöz;

- adatok, eszközök eltulajdonítását, visszaélésszerű felhasználását;
- megtévesztő adatok bevitelét és képzését;
- eszközök, adathordozók megrongálását, működésük, használhatóságuk korlátozását;
- feldolgozások és munkafolyamatok zavarását, késleltetését;
- vírusfertőzött adathordozó szándékos behozatalát, vírusfertőzés előidézését;
- illegális szoftverek telepítését;
- a törvények és szabályok tudatos vagy szándékos megsértését.

A Szervezet gondatlan károkozásnak tekinti az alábbiakat:

- figyelmetlenséget, az ellenőrzés elmulasztását;
- szakmai hozzá nem értést, a kötelezően elvárható gondosság és előrelátás hiányát, elmulasztását;
- megváltozott működési körülményeknek figyelmen kívül hagyását;
- biztonsági követelmények és gyári előírások be nem tartását;
- adathordozók megrongálódását az előírásoktól eltérő tárolás és kezelés miatt;
- karbantartási műveletek elmulasztását;
- biztonsági-, jelző- és riasztóberendezések karbantartásának elhanyagolását;
- eszköz és eljárásbeli biztosítékok informatikai rendszerekbe történő beépítésének elhanyagolását.

Az IBF a tudomására jutott események súlyosságát mérlegeli, és szándékos, illetve gondatlan károkozás esetén jelenti az informatikai vezetőnek.

Az információbiztonsági előírások megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor, amelyet az IBF jelentése alapján az informatikai vezető kezdeményezhet. Az eljárást a jogszabályok és a Szervezet belső szabályzatai szerint kell lefolytatni.

Amennyiben a biztonsági előírásokat külső partner sérti meg, a szerződésben rögzített következmények érvényesítésével kell elérni az előírások betartását.

3.1.6.7.1.1. ELJÁRÁSREND

A Szervezet belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben. Az eljárást az erre kijelölt etikai bizottság folytatja le.

3.1.6.7.1.2. JOGI ESZKÖZÖK

Ha az elektronikus információbiztonsági szabályokat nem a Szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

3.1.6.8. BELSŐ EGYEZTETÉS

A Szervezet tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

3.1.6.9. VISELKEDÉSI SZABÁLYOK AZ INTERNETEN

A Szervezet alkalmazottai amennyiben munkájuk indokolja, hozzáférést kaphatnak az Internethez. A hozzáférés kiadása történhet meghatározott szervezeti egységek számára mindenkire vonatkozóan, vagy egyénileg igényelve a jogosultságok igényelésének eljárása szerint.

Az Internet használatának kizárólagos célja a munkavégzés. A felhasználó nem jogosult magáncélra használni a web elérését.

A hálózat nem használható az alábbi módon, az alábbi tevékenységekre:

a) A hatályos magyar törvényekbe ütköző cselekmények, ideértve, de nem korlátozva azokra: mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; szoftver szándékos és tudatos illegális terjesztése.

b) A hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, a mennyiben ezek a tevékenységek ezen hálózatokat érintik.

c) Profitszerzést célzó direkt üzleti célú tevékenység (pl. bérletöltés), reklámok terjesztése.

d) A hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység (idegen jelszó kiderítése saját és idegen hálózatban, idegen felhasználói név használata az illető tudomása nélkül).

e) A hálózatot, illetve erőforrásait indokolatlanul vagy szándékosan túlzott mértékben, pazarló módon igénybe vevő tevékenység (pl. levélbombák, elektronikus játékok).

f) A hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, törlése.

g) A hálózat biztonságát veszélyeztető információk, programok terjesztése.

h) Mások személyiségi jogait, vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység (pl. pornográf anyagok közzététele).

i) Mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása (pl. kéretlen levelek).

j) Tilos az Interneten keresztül belső használatú, bizalmas vagy titkos dokumentumokat, adatokat a Szervezetből engedély nélkül kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni.

A lokális (belső) hálózatra vonatkozó általános szabályok azonosak az internetre vonatkozó szabályokkal, kiegészítve azzal, hogy a tiltott magatartási formák előkészítése, illetve kísérlete is szankcionálható.

AZ INTERNET HOZZÁFÉRÉS BIZTONSÁGI ELŐÍRÁSAI

Az Internet hozzáférés a Szervezet informatikai rendszereinek biztonságára nézve az egyik fő veszélyforrás, ezért az Internet hozzáférés biztonsága érdekében az alábbi előírásokat kell betartani:

A számítógépre telepített, naprakész (legalább naponta frissülő) vírusadatbázissal rendelkező vírusvédelmi szoftver nélkül tilos az Internetet használni. Jelenteni kell a HelpDesk-en, ha valamilyen oknál fogva a számítógépen nem fut vírusvédelmi szoftver, vagy nem frissül a vírusdefiníciós adatbázisa és a szoftver azt jelzi, hogy az adatbázis elavult.

Tilos gyanús (pl. illegális szoftvereket vagy erotikus tartalmat kínáló) webhelyekről fájlokat letölteni. Internetezés közben azonnal el kell hagyni azokat a webhelyeket, amelyekre vonatkozóan a vírusvédelmi szoftver vagy az webböngésző vírusveszélyre, vagy adatok megszerzésére vonatkozó tevékenységre (adathalászatra) figyelmeztet.

Az Internetről letöltött fájlok vírusokat tartalmazhatnak. Mivel a vírusvédelmi szoftverek nem ismernek fel azonnal minden új vírust vagy vírusváltozatot, a számítógép akkor is megfertőződhet, ha naprakész a vírusvédelmi szoftver vírusadatbázisa, ezért a letöltött fájlok megnyitásakor mindig óvatosan kell eljárni.

Internetezés közben el kell utasítani azokat a felbukkanó ablakokat, amelyek segédprogramok telepítését, vagy egyes biztonsági funkciók kikapcsolását kezdeményezik.

Tilos az Internet zóna biztonsági szintjét közepesnél alacsonyabbra állítani az webböngésző beállításaiban.

Tilos a webhelyek eléréséhez szükséges jelszavakat úgy megválasztani, hogy abból a Szervezetnél használt jelszóra következtetni lehessen.

Javasolt az Internetről letöltött átmeneti fájlok és a felkeresett webhelyek által létrehozott fájlok (cookie-k) rendszeres törlése.

KORLÁTOZÁSOK AZ INTERNET HASZNÁLATÁBAN

A Szervezetnél csak a rendszeresített internetes alkalmazások használhatók.

A Szervezet fenntartja a jogot a fájltípustól (pl.: .avi, .mpg, .wmv kiterjesztésű fájlok), valamint mérettől függő letöltés korlátozására, illetve bizonyos típusú, a napi munkát nem támogató webhelyekhez való hozzáférés megakadályozására.

AZ INTERNET HOZZÁFÉRÉSEK ELLENŐRZÉSE

A Szervezet fenntartja a jogot a felhasználók Internet forgalmának naplózására, az internetezés gyakoriságának, és ha szükséges tartalmának ellenőrzésére, korlátozására az Internet kapcsolat sávszélességének hatékonyabb kihasználása, valamint a Szervezet informatikai rendszereinek biztonsága érdekében.

A fenti ellenőrzéseket az üzemeltető, vagy az IT csoport felsővezetői, vagy IBF kérése esetén végzi.

3.1.6.9.1.1. INFORMÁCIÓK NYILVÁNOSSÁGA

A Szervezet tiltja és számonkéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét.

HONLAP

Az Szervezet hivatalos honlapja

https://kszki.hu

A honlap karbantartását a Szervezet munkatársai (portálgazda) végzik külön utasítás alapján.

3.1.6.9.1.2. TILTOTT TEVÉKENYSÉGEK

a) Tilos olyan tevékenységet kifejteni, amely célja mások adatainak jogosulatlan megszerzése, megváltoztatása, letörlése.

b) Tilos más felhasználók nevében tevékenykedni.

c) A felhasználó nem teheti lehetővé mások számára, hogy a nevében tevékenykedjenek. Ezért – többek

között – mindent meg kell tennie a jelszavai titkosságának megőrzése érdekében, továbbá ezért, hogy a személyazonosító eszközeit (például, de nem kizárólag: VPN kulcs, azonosító kártya, mobil telefon) más ne használhassa.

d) A felhasználó köteles törekedni arra, hogy az általa pillanatnyilag használatba vett rendszerekben más személy ne fejthessen ki aktivitást.

e) Tilos más munkavégzését korlátozó tevékenységet végezni nem munka céljából kifejtett aktivitással.

f) Tilos a rendszer bármely elemének eredeti felhasználási céljától eltérő használata vagy az erre irányuló próbálkozás.

g) Tilos a Szervezet rendszergazdájától kapott IP címtől eltérő más IP cím jogosulatlan használata.

h) Tilos olyan anyag továbbítása, letöltése vagy közzététele az interneten, amely a Magyar és Uniós törvényeket sérti.

i) Tilos a Szervezet belső informatikai rendszerén kívüli helyszínről elérni vagy megpróbálni elérni a rendszert, kivéve, ha erre az IT csoport engedélyt ad.

j) Tilos külső személy számára információt adni a rendszer valamely hibájáról, sebezhető pontjáról.

3.1.6.9.1.3. SZERVEZETTŐL IDEGEN TEVÉKENYSÉGEK

A Szervezet tiltja a közösségi oldalak használatát, magánpostafiók mellékleteinek, csatolmányainak elérését, és más, a szervezettől idegen tevékenységet.

3.1.7 TUDATOSSÁG ÉS KÉPZÉS

3.1.7.1. KAPCSOLATTARTÁS

A Szervezet kapcsolatot tart az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel az IBF-en keresztül.

3.1.7.1.1.1. FOLYAMATOS KÉPZÉS

A Szervezet az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek folyamatos oktatásának, képzésének elősegítésére törekszik.

3.1.7.1.1.2. NAPRAKÉSZSÉG

A Szervezet az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása érdekében minden rendelkezésére álló erőforrást igénybe vesz.

3.1.7.1.1.3. INFORMÁCIÓCSERE

A Szervezet a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel, továbbá a tevékenysége körében meghatározott szakmai céllal létrejövő fórumokon.

3.1.7.2. KÉPZÉSI ELJÁRÁSREND

3.1.7.2.1.1. KIHIRDETÉS

A képzési eljárásrend kihirdetési eljárása megegyezik az Informatikai Biztonsági Szabályzat kihirdetésének módjával.

3.1.7.2.1.2. FELÜLVIZSGÁLAT

A képzési eljárásrend felülvizsgálata és frissítésének gyakorisága azonos az Informatikai Biztonsági Szabályzat eljárásaival.

3.1.7.3. BIZTONSÁG TUDATOSSÁG KÉPZÉS

3.1.7.3.1. FELHASZNÁLÓK KÉPZÉSE

A Szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára.

3.1.7.3.1.1. ÚJ FELHASZNÁLÓK

Az új felhasználók kezdeti képzésének részeként, a munka megkezdése előtt képzést szervez, és nyilatkozatot kér a szabályzat elfogadásáról.

3.1.7.3.1.2. VÁLTOZÁS

A Szervezet, amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi, haladéktalanul kiegészítő képzést szervez a felhasználóknak.

3.1.7.3.1.3. RENDSZERESSÉG

A képzéseket legalább évente meg kell tartani, és dokumentálni.

3.1.7.5. SZEREPKÖR, VAGY FELADAT ALAPÚ BIZTONSÁGI KÉPZÉS

3.1.7.5.1. SZEREPKÖRÖK SZERINTI KÉPZÉS

A Szervezet szerepkör, vagy feladat alapú biztonsági képzést nyújt az egyes szerepkörök szerinti, azért felelős személyeknek.

3.1.7.5.1.1. ELŐZETES FELKÉSZÜLÉS

A Szervezet az elektronikus információs rendszerhez való hozzáférés engedélyezését, vagy a kijelölt feladat végrehajtását megelőzően is nyújt képzéseket.

3.1.7.5.1.2. VÁLTOZÁS

A Szervezet, amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi, haladéktalanul kiegészítő szakképzést szervez a felhasználóknak.

3.1.7.5.1.3. RENDSZERESSÉG

A képzéseket legalább három évente meg kell tartani, és dokumentálni.

3.1.7.6. A BIZTONSÁGI KÉPZÉSRE VONATKOZÓ DOKUMENTÁCIÓK

3.1.7.6.1.1. KÉPZÉSEK DOKUMENTÁLÁSA

A Szervezet dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket. A dokumentumok tartalmazzák:

- Az oktatás tematikáját
- Az oktatás anyagait (ppt)
- Az oktatás helyét és idejét
- A résztvevők felsorolását és aláírását
- Az oktató megnevezését, és aláírását.

3.1.7.6.1.2. A DOKUMENTUMOK MEGŐRZÉSE

A Szervezet a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és a dokumentumokat megőrzi, legalább 5 évig.

MELLÉKELTEK

1. SZ. MELLÉKLET: BIZTONSÁGI ESEMÉNYEK KIVIZSGÁLÁSA

Változat: 1

Kivizsgálás részletei (informatikai biztonsági felelős tölti ki):

HelpDesk bejelentés száma:	
Szervezet neve:	
Észlelő neve:	
Informatikai rendszer:	
Esemény fajtája:	
Tapasztalás helye, ideje:	
Esemény leírása:	
Kivizsgálás leírása:	
Végzett / javasolt intézkedés leírása:	
Intézkedés életbelépésének dátuma:	
Végleges-e az intézkedés:	☐ Igen ☐ Nem
Igényel-e kockázatelemzést:	☐ Igen ☐ Nem
Kivizsgálás dátuma:	
Kivizsgáló neve, aláírása [1]:	

Kivizsgálás jóváhagyása (informatikai vezető tölti ki):

Jóváhagyás:	☐ Jóváhagyva ☐ Elutasítva ☐ Kiegészítéssel jóváhagyva
Jóváhagyó megjegyzése (elutasítás indoklása, kiegészítések):	
Jóváhagyó neve, aláírása [1]:	

[1] **Az űrlapot elektronikusan kérjük kitölteni és lementeni.** Az adott személytől e-mail-ben érkező, elektronikusan kitöltött űrlapot aláírás nélkül is érvényesnek tekintjük. A lezárt űrlapot PDF formátumban kell megőrizni.

2. SZ. MELLÉKLET: FIZIKAI BELÉPÉSI KÉRELEM

Változat: 1

Belépési engedély alanyának adatai (munkahelyi vezető tölti ki):

Szervezet neve:	
Belépési engedély alanyának neve (a beosztott munkatárs, akire az igénylés vonatkozik):	
Dolgozó kód:	
Elérhetőség (e-mail vagy telefon):	

Igényelt művelet (munkahelyi vezető tölti ki):

Igénylés típusa:	☐ Engedély kiadása	☐ Visszavonása
Belépési engedély kezdete, vége:		
Igényelt telephelyek / védett területek (szerverterem, hálózati rendező helyiség, hálózati rack szekrények):		
Belépési igény indoklása (az igényléshez kapcsolódó feladatellátás megnevezése):		
Igénylés dátuma:		
Munkahelyi vezető neve, aláírása [1]:		

[1] **Az űrlapot elektronikusan kérjük kitölteni és lementeni**, majd a portaszolgálatnak e-mail-ben elküldeni.
Az adott személytől e-mail-ben érkező, elektronikusan kitöltött űrlapot aláírás nélkül is érvényesnek tekintjük.

Védett területhez hozzáférés jóváhagyása (védett területhez tartozó szervezeti egység vezetője tölti ki):

Védett terület(ek):		
Jóváhagyás:	☐ Jóváhagyva	☐ Elutasítva
Jóváhagyó neve, aláírása [2]:		

Védett területhez hozzáférés jóváhagyása (védett területhez tartozó szervezeti egység vezetője tölti ki):

Védett terület(ek):		
Jóváhagyás:	☐ Jóváhagyva	☐ Elutasítva
Jóváhagyó neve, aláírása [2]:		

[2] **Az űrlapot elektronikusan kérjük kitölteni és lementeni**, majd a portaszolgálatnak e-mail-ben visszaküldeni. Az adott személytől e-mail-ben érkező, elektronikusan kitöltött űrlapot aláírás nélkül is érvényesnek tekintjük.

Belépési engedély kiadása (portaszolgálat tölti ki):

Engedély kiadás dátuma:	
Engedélyt kiadó neve, aláírása [3]:	

[3] **Az űrlapot elektronikusan kérjük kitölteni és lementeni**, majd a lezárt űrlapot PDF formátumban megőrizni. Az elektronikusan kitöltött és PDF formátumban lementett űrlapot aláírás nélkül is érvényesnek tekintjük.

3. SZ. MELLÉKLET: BELÉPÉSI NAPLÓ

Napló sorszáma: ..... Változat: 1

Telephely / védett terület:				
Belépő neve	**Szervezete**	**Belépés dátuma**	**Belépés ideje** [1]	**Kilépés ideje** [1]

[1] Védett területek esetén a kulcs felvételének és leadásának ideje.

4. SZ. MELLÉKLET: VÁLTOZTATÁSI KÉRELEM

Változat: 1

Változtatási igény részletei (változtatást kezdeményező tölti ki):

Informatikai rendszer:	
Változtatás tárgya (érintett hardver/szoftver rendszerelemek):	
Változtatás rövid megnevezése:	
Tervezett változtatás leírása:	
Változtatás tervezett dátuma és időpontja:	
Igénylés dátuma:	
Igénylő neve, aláírása [1]:	

Adatgazdai terület jóváhagyása (adatgazdai terület vezetője vagy a kulcsfelhasználó tölti ki):

Jóváhagyás:	☐ Jóváhagyva ☐ Elutasítva ☐ Kiegészítéssel jóváhagyva
Jóváhagyó megjegyzése (elutasítás indoklása, kiegészítések):	
Jóváhagyó neve, aláírása [1]:	

Informatikai terület jóváhagyása (informatikai terület vezetője tölti ki):

Jóváhagyás:	☐ Jóváhagyva ☐ Elutasítva ☐ Kiegészítéssel jóváhagyva
Jóváhagyó megjegyzése (elutasítás indoklása, kiegészítések):	
Jóváhagyó neve, aláírása [1]:	

Informatikai biztonsági felelős jóváhagyása [2]:

Jóváhagyás:	☐ Jóváhagyva ☐ Elutasítva ☐ Kiegészítéssel jóváhagyva
Jóváhagyó megjegyzése (elutasítás indoklása, kiegészítések):	
Jóváhagyó neve, aláírása [1]:	

[2] Kisebb verzióváltások, a gyártó által kiadott frissítések telepítése esetén nem szükséges az IBF jóváhagyása.

Változtatás kivitelezése (változtatást végző tölti ki):

Elvégzett változtatás leírása és a változtatást követő teszt leírása:		
Teszt eredménye:	☐ Megfelelt	☐ Nem felelt meg
Változtatás dátuma:		
Változtatást végző neve, aláírása [1]:		

[1] **Az űrlapot elektronikusan kérjük kitölteni és lementeni**. Az adott személytől e-mail-ben érkező, elektronikusan kitöltött űrlapot aláírás nélkül is érvényesnek tekintjük. A lezárt űrlapot PDF formátumban kell megőrizni.

5. SZ. MELLÉKLET: TESZTELÉSI JEGYZŐKÖNYV

Változat: 1

Tesztelés részletei (tesztelést végző tölti ki):

Tesztelés tárgya (informatikai rendszer / hardver/szoftver elemek megnevezése):		
Tesztelés célja:		
Teszteléshez igénybe vett eszközök (hardver / szoftver megnevezése, típusa):		
Alkalmazott módszer (beállítási paraméterek és körülmények, egyéb információk):		
Teszt leírása (konkrét teszteredmények, következtetés):		
Teszt eredménye:	☐ Megfelelt	☐ Nem felelt meg
Nem megfelelőség kiküszöbölése (tett javaslatok, észrevételek):		
Tesztelés dátuma:		
Tesztelést végző neve, aláírása [1]:		

Tesztelés eredményének jóváhagyása (tesztelést jóváhagyó vezető tölti ki):

Jóváhagyás:	☐ Jóváhagyva ☐ Kiegészítéssel jóváhagyva	☐ Elutasítva
Jóváhagyó megjegyzése (elutasítás indoklása, kiegészítések):		
Jóváhagyó neve, aláírása [1]:		

[1] **Az űrlapot elektronikusan kérjük kitölteni és lementeni**. Az adott személytől e-mail-ben érkező, elektronikusan kitöltött űrlapot aláírás nélkül is érvényesnek tekintjük. A lezárt űrlapot PDF formátumban kell megőrizni.

6. SZ. MELLÉKLET: HOZZÁFÉRÉSI JOGOSULTSÁG IGÉNYLŐ

Változat: 1

Jogosultság alanyának adatai (munkahelyi vezető tölti ki):

Szervezet neve:	
Jogosultság alanyának neve (a beosztott munkatárs, akire az igénylés vonatkozik):	
Dolgozó kód (új hozzáférés esetén kötelező kitölteni):	
Felhasználói azonosító (meglévő hozzáférés esetén kötelező kitölteni):	
Személyes e-mail vagy mobiltelefon (ahová a felhasználói azonosító és a kezdeti jelszó küldhető; új hozzáférés esetén kötelező kitölteni):	

Igényelt jogosultság részletei (munkahelyi vezető tölti ki):

Informatikai rendszer:			
Igénylés típusa:	☐ Új hozzáférés	☐ Módosítás	☐ Visszavonás
	☐ Felhasználó letiltása	☐ Letiltott felhasználó engedélyezése	
Igényelt / visszavonandó jogosultságok (a létező jogosultsági csoportokból választva):			
Megjegyzés (szövegesen megfogalmazott jogosultsági igény):			
Ugyanaz a jogosultság, mint (új hozzáférés és módosítás esetén, a jogosultságok megadása helyett kérhető az adott felhasználóval egyező jogosultság):			
Jogosultságigény indoklása (az igényléshez kapcsolódó feladatellátás megnevezése):			
Jogosultság kezdete, vége (ha nincs kitöltve, a jogosultság a kiadás dátumától határozatlan időre szól):			
Igénylés dátuma:			
Munkahelyi vezető neve, aláírása [1]:			

Jogosultság engedélyezése (kulcsfelhasználó tölti ki):

Engedélyezés:	☐ Engedélyezve ☐ Elutasítva ☐ Módosított jogosultságokkal engedélyezve
Engedélyező megjegyzése (elutasítás indoklása, módosított jogosultságok):	
Engedélyező neve, aláírása [2]:	

Jogosultság beállítása (rendszergazda tölti ki):

Kiadott felhasználói azonosító (új hozzáférés esetén):	
Jogosultságot kiadó megjegyzése (ténylegesen kiadott jogosultságok):	
Jogosultság kiadás dátuma:	
Jogosultságot kiadó neve, aláírása [3]:	
Jogosultság visszavonás dátuma [4]:	
Jogosultságot visszavonó neve, aláírása [3]:	

7. SZ. MELLÉKLET: HÁLÓZATI JOGOSULTSÁG IGÉNYLŐ

Változat: 1

Jogosultság alanyának adatai (munkahelyi vezető tölti ki):

Szervezet neve:		
Jogosultság alanyának neve (a beosztott munkatárs, akire az igénylés vonatkozik):		
Dolgozó kód (új hozzáférés esetén kötelező kitölteni):		
Felhasználói azonosító (meglévő hozzáférés esetén kötelező kitölteni):		
Beosztás [1]:		
Szervezeti egység [1]:		
Mobiltelefon [1]:		
Vezetékes telefon / mellék [1]:		
Személyes e-mail vagy mobiltelefon (ahová a felhasználói azonosító és a kezdeti jelszó küldhető; új hozzáférés esetén kötelező kitölteni):		

Igényelt jogosultság részletei (munkahelyi vezető tölti ki):

Hálózati szolgáltatások:	☐ Hálózati hozzáférés ☐ Internet hozzáférés	☐ Elektronikus levelezés	
Igénylés típusa:	☐ Új hozzáférés ☐ Felhasználó letiltása	☐ Módosítás ☐ Letiltott felhasználó engedélyezése	☐ Visszavonás
Igényelt / visszavonandó jogosultságok hálózati mappákhoz (a létező jogosultsági csoportokból választva): **Megjegyzés** (szövegesen megfogalmazott jogosultsági igény):			
Ugyanaz a jogosultság, mint (új hozzáférés és módosítás esetén, a jogosultságok megadása helyett kérhető az adott felhasználóval egyező jogosultság):			
Jogosultságigény indoklása (az igényléshez kapcsolódó feladatellátás megnevezése):			

Jogosultság kezdete, vége (ha nincs kitöltve, a jogosultság a kiadás dátumától határozatlan időre szól):		
Igénylés dátuma:		
Munkahelyi vezető neve, aláírása [2]:		

Hálózati mappák jogosultság engedélyezése (hálózati mappához tartozó szervezeti egység vezetője tölti ki):

Hálózati mappá(k):	
Engedélyezés:	☐ Engedélyezve ☐ Elutasítva ☐ Módosított jogosultságokkal engedélyezve
Engedélyező megjegyzése (elutasítás indoklása, módosított jogosultságok):	
Engedélyező neve, aláírása [3]:	

Hálózati mappák jogosultság engedélyezése (hálózati mappához tartozó szervezeti egység vezetője tölti ki):

Hálózati mappá(k):	
Engedélyezés:	☐ Engedélyezve ☐ Elutasítva ☐ Módosított jogosultságokkal engedélyezve
Engedélyező megjegyzése (elutasítás indoklása, módosított jogosultságok):	
Engedélyező neve, aláírása [3]:	

Hálózati mappák jogosultság engedélyezése (hálózati mappához tartozó szervezeti egység vezetője tölti ki):

Hálózati mappá(k):	
Engedélyezés:	☐ Engedélyezve ☐ Elutasítva ☐ Módosított jogosultságokkal engedélyezve
Engedélyező megjegyzése (elutasítás indoklása, módosított jogosultságok):	
Engedélyező neve, aláírása [3]:	

Hálózati mappák jogosultság engedélyezése (hálózati mappához tartozó szervezeti egység vezetője tölti ki):

Hálózati mappá(k):	
Engedélyezés:	☐ Engedélyezve ☐ Elutasítva ☐ Módosított jogosultságokkal engedélyezve
Engedélyező megjegyzése (elutasítás indoklása, módosított jogosultságok):	
Engedélyező neve, aláírása [3]:	

Hálózati mappák jogosultság engedélyezése (hálózati mappához tartozó szervezeti egység vezetője tölti ki):

Hálózati mappá(k):	
Engedélyezés:	☐ Engedélyezve ☐ Elutasítva ☐ Módosított jogosultságokkal engedélyezve
Engedélyező megjegyzése (elutasítás indoklása, módosított jogosultságok):	
Engedélyező neve, aláírása [3]:	

Hálózati mappák jogosultság engedélyezése (hálózati mappához tartozó szervezeti egység vezetője tölti ki):

Hálózati mappá(k):	
Engedélyezés:	☐ Engedélyezve ☐ Elutasítva ☐ Módosított jogosultságokkal engedélyezve
Engedélyező megjegyzése (elutasítás indoklása, módosított jogosultságok):	
Engedélyező neve, aláírása [3]:	

Jogosultság beállítása (rendszergazda tölti ki):

Kiadott felhasználói azonosító (új hozzáférés esetén):	
Kiadott e-mail cím (új hozzáférés esetén):	
Jogosultságot kiadó megjegyzése (ténylegesen kiadott jogosultságok):	
Jogosultság kiadás dátuma:	
Jogosultságot kiadó neve, aláírása [4]:	
Jogosultság visszavonás dátuma [5]:	
Jogosultságot visszavonó neve, aláírása [4]:	

8. SZ. MELLÉKLET: KARBANTARTÁSI NAPLÓ

Változat: 1

Karbantartás engedélyezése (informatikai terület vezetője tölti ki):

Informatikai rendszer(ek):	
Karbantartás tárgya (érintett hardver/szoftver rendszerelemek):	
Karbantartás rövid megnevezése:	
Karbantartás dátuma, időpontja:	
Karbantartás tervezett időtartama:	
Karbantartás elrendelt végzője:	
Engedélyezés dátuma:	
Engedélyező neve, aláírása [1]:	

Karbantartás elvégzése (karbantartást végző tölti ki):

Elvégzett karbantartás és a karbantartást követő teszt leírása:		
Teszt eredménye:	☐ Megfelelt	☐ Nem felelt meg
Karbantartás tényleges időtartama:		
Leállási idő (ha volt ilyen):		
Karbantartást végző neve, aláírása [1]:		

9. SZ. MELLÉKLET: ÜZEMBE HELYEZÉSI JEGYZŐKÖNYV

Változat: 1

Üzembe helyezés adatai:

Üzembe helyezés jellege:	☐ Számítógép / egyéb eszköz első üzembe behelyezése ☐ Áthelyezés (tárolóhely / felhasználó változása) ☐ Tartozékok üzembe helyezése / eltávolítása ☐ Szoftverek telepítése / eltávolítása
Üzembe helyezés dátuma:	
Üzembe helyező neve, aláírása:	

Számítógép / egyéb eszköz alapadatok:

Szervezet neve:	
Informatikai azonosító:	
Leltári szám:	
Eszköz csoportja (pl. asztali számítógép, laptop, hálózati nyomtató):	
Eszköz gyártója, típusa:	
Tárolóhely (tárolóhely kód és megnevezés vagy telephely, épület, emelet, szoba):	
Új tárolóhely (változás esetén):	
Eszközért felelős felhasználó:	
Új felelős felhasználó (változás esetén):	
Eszköz rövid megnevezése (ha nem egyezik meg a felhasználó nevével, pl. közös használatú vagy speciális célú számítógépek esetén):	
Új eszköz megnevezés (változás esetén):	

Eszköz tartozékok (anyagként kezelt tartozékok pl. billentyűzet, egér, hangszóró nélkül):

Inform. azonosító	**Leltári szám**	**Tartozék csoportja** (pl. monitor, nyomtató)	**Tartozék gyártója, típusa**	**Üzembe helyezve**	**Eltávolítva**
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐

Inform. azonosító	**Leltári szám**	**Tartozék csoportja** (pl. monitor, nyomtató)	**Tartozék gyártója, típusa**	**Üzembe helyezve**	**Eltávolítva**
				☐	☐
				☐	☐
				☐	☐

Licenc köteles szoftverek (szabad szoftverek nélkül):

Szoftver neve és verziószáma	**Telepítve**	**Eltávolítva**
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐

FELHASZNÁLÓI NYILATKOZAT:

Kijelentem, hogy a számítógépet és tartozékait üzemszerű állapotban átvettem, az eszközöket rendeltetésszerűen használom, azokat önkényesen nem helyezem át, további szoftvereket nem telepítek.

Tudomásul veszem, hogy az Informatikai Biztonsági Szabályzat alapján az **illegális szoftvertelepítés szándékos károkozásnak minősül** és az előírás megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor.

A működésbeli meghibásodásokat, az eszközök áthelyezési igényét az Informatikai Biztonsági Szabályzatnak megfelelően a Helpdesk-en jelentem az IT csoportnak.

Dátum: 20…… / …… / ……

……

Eszközért felelős felhasználó

10. SZ. MELLÉKLET: BIZTONSÁGI OSZTÁLYBA ÉS SZINTBE SOROLÁS[1]

A biztonsági szint: 3 (Lásd: Szintbesorolás és védelmi intézkedés űrlap)

A biztonsági osztályba sorolások külön dokumentumban találhatók (OVI lapok)

ALAPFOGALMAK

információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.

adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

személyes adat: meghatározott természetes személlyel kapcsolatba hozható adat, az adatból levonható, a személyre vonatkozó következtetés.

különleges adat: faji eredetre, nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, szexuális életre, egészségi állapotra, kóros szenvedélyre, büntetett előéletre vonatkozó személyes adat.

kritikus adat: személyes adat, különleges adat vagy valamely jogszabállyal védett adat (pl.: adó-, orvosi-, ügyvédi-, biztosítási-, banktitok stb.).

adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése.

adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.

adatkezelő: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

adatfeldolgozó: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.

szervezet: az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető.

üzemeltető: az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer, vagy annak részei működtetését végzi és a működésért felelős.

elektronikus információs rendszer (jelen szabályzatban röviden: **informatikai rendszer**): az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.

bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (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: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

fenyegetés, fenyegető tényező: olyan lehetséges művelet, esemény vagy mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer vagy elemeinek védettségét, biztonságát.

sérülékenység, gyenge pont: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.

sérülékenységvizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.

kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása.

biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.

biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége.

biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása.

biztonsági szint: a szervezet felkészültsége az Ibtv. törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

biztonsági szintbe sorolás: a szervezet felkészültségének meghatározása az Ibtv. törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.

fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.

logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.

kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

biztonsági audit: az információbiztonsági előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés.

Informatikai fogalmak

hardver: a számítógép, az informatikai rendszer fizikai elemei.

szerver: olyan számítógépek vagy egyéb eszközök, illetve szoftverek, amelyek különböző szolgáltatásokat biztosítanak más számítógépek/hardver eszközök, illetve szoftverek (általánosan: kliensek) számára.

kliens: olyan számítógépek vagy egyéb eszközök, illetve szoftverek, amelyek a szerverek szolgáltatásait használják.

fizikai szerver: egy fizikailag létező, szerver funkciót ellátó számítógép vagy egyéb eszköz.

virtuális szerver: a fizikai szerveren (annak erőforrásainak felhasználásával) logikailag létrehozott szerver, amely a kliensek számára a fizikai szerverekkel azonos funkcionalitású. A virtuális szerverek a rendelkezésre állási szint növelése érdekében manuálisan vagy automatizáltan mozgathatóak a fizikai szerverek között.

szerverterem: fokozottan védett, általában naplózott bejutású, légkondicionált, zárt helyiség, ahol biztosítottak a folyamatos működés feltételei a szerverek, központi hálózati eszközök számára.

rack szekrény: informatikai eszközök elhelyezésére szolgáló, szabványos méretű egységekből (unitokból) álló, zárható szekrény, mely tartalmazza az eszközök és berendezések fizikai rögzítéséhez, a különféle kábelek elrendezéséhez szükséges szerelvényeket.

szoftver: a számítógép, az informatikai rendszer logikai elemei; a rendszerszoftverek (pl. operációs rendszerek) és az alkalmazói szoftverek (alkalmazások) összefoglaló neve.

program: számítógépes utasítások logikailag és funkcionálisan összetartozó sorozata. Állhat egyetlen programmodulból vagy programmodulok halmazából.

alkalmazói szoftver, alkalmazás: olyan program, amelyet a felhasználó a saját igényei, céljai érdekében használ, és amely a rendszerszoftverek által biztosított funkcióikat használja.

rendszerszoftver: olyan alapszoftver (pl.: operációs rendszer, adatbáziskezelő szoftver, tűzfal szoftver stb.), amelyre szükség van az informatikai rendszer hardver elemeinek használatához és az alkalmazói szoftverek működtetéséhez.

operációs rendszer: olyan rendszerszoftver, amely ellenőrzi a számítógép alapvető műveleteit, az adatbevitelre, megjelenítésre, adattárolásra, adatátvitelre szolgáló hardver egységeket, lehetővé teszi a felhasználóval történő kapcsolattartást és az alkalmazói szoftverek futtatását.

vírus: olyan általában károkozási szándékkal létrehozott program, amely képes önmagát reprodukálva valamilyen hordozó közegen keresztül (pl. futtatható fájlok vagy makrókat tartalmazó dokumentumok felhasználásával) terjedni és más számítógépeket „megfertőzni”.

makró vírus: olyan dokumentumhoz csatolt (abban tárolt) makrónyelven írt vírus, amely a dokumentumot kezelő és a makrót használni képes alkalmazói szoftverhez kötődik. Hatását a dokumentum használata során fejti ki.

féreg: olyan vírushoz hasonló károkozó program, amely terjedéséhez nincs szükség a vírusokra jellemző hordozó közegre, amely a hálózaton keresztül, a hálózati funkciók kihasználásával terjed.

kémprogram: olyan kártékony program, amely feladata a számítógépen tárolt bizalmas adatok (pl.: jelszavak, kódok, bankkártya- és személyes adatok) megszerzése és továbbítása.

trójai program: olyan hasznosnak álcázott program, amely magában nem okoz kárt, de képes a háttérben segíteni egyéb kártékony programok bejutását és működését a számítógépen.

szoftverlicenc: az adott szoftver szerzői jogtulajdonosa által szerződésben meghatározott, a szoftver használatára vonatkozó feltételeket tartalmazó használati engedély. A jogilag tisztázott, legális szoftverhasználatot a szoftver licencének rendelkezésre állásával lehet bizonyítani.

OEM licenc: valamilyen informatikai eszköz vagy alkatrész megvásárlásához kötött szoftverlicenc, mely egyértelműen kötődik az adott eszközhöz/alkatrészhez, csak azzal együtt használható.

hálózat: a kliens számítógépek és a szerverek közötti adatátvitelt biztosító passzív és aktív hálózati eszközökből álló infrastruktúra.

passzív hálózati eszközök: a hálózati kábelezés és a csatlakozók.

aktív hálózati eszközök: kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok (access point-ok) és egyéb eszközök, amelyek segítségével a hálózat működése biztosítható.

tűzfal: olyan eszköz (speciális hálózati eszköz vagy szoftver), amelyet a belső és a külső hálózat közé, a csatlakozási pontra telepítenek, annak érdekében, hogy az illetéktelen behatolásoknak elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is.

WiFi: szabványos, vezeték nélküli, rádiófrekvenciás adatátviteli technika. A legtöbb mobil eszköz (pl.: laptop, mobiltelefon, PDA, táblagép) gyárilag rendelkezik ilyen kapcsolódási lehetőséggel.

virtuális helyi hálózat, VLAN: a helyi hálózat logikai alapon szervezett, elkülönített része, amelybe fizikai elhelyezkedéstől függetlenül tartozhatnak bele az eszközök.

virtuális magánhálózat, VPN: nyilvános hálózat (pl. Internet) egyes végpontjai között kiépített logikai hálózat, amelyen keresztülmenő adatok nem láthatók az eredeti hálózaton, mivel titkosított adatcsomagokba vannak becsomagolva.

protokoll: az informatikai eszközök, illetve szoftverek közötti kommunikáció módját leíró szabályok gyűjteménye.

Domain Name System, DNS: olyan rendszer, amely az Interneten vagy a belső hálózaton a számítógépekhez, egyéb eszközökhöz vagy szolgáltatásokhoz tartozó, az emberek számára értelmes neveket (pl. www.kszki.hu) a hálózati eszközök számára érthető címekre (IP címekre) „fordítja le”, „oldja fel”, melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton.

intranet: a Szervezeten belüli hálózat és annak szolgáltatásai.

Internet: nyilvános, világméretű számítógépes hálózat, amely szolgáltatások széles skáláját (pl.: www, e-mail, ftp, stb.) nyújtja felhasználóinak.

webböngésző: olyan program, amellyel az Interneten található tartalmakat – legtöbbször weboldalakat – lehet megtekinteni, illetve az Interneten keresztül elérhető szolgáltatásokat használni.

weboldal, weblap: egy olyan webdokumentum, mely megfelel a World Wide Web szabványoknak, és alkalmas arra, hogy egy webböngésző megjelenítse.

webhely, website: egy adott Internet címen (domain-en) található weboldalak összessége.

felhasználó: az informatikai rendszereket igénybe vevő, használó természetes személy.

felhasználói azonosító: a felhasználó egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó nevéből képződik.

felhasználói fiók: a felhasználó adott informatikai rendszerhez történő hozzáférését reprezentáló adatok összessége: a felhasználói azonosító, a jelszó, a hozzáférési jogosultságok és egyéb adatok, illetve beállítások.

jelszó: a felhasználóhoz kötődő egyedi titkos karaktersorozat, mely a felhasználó hitelesítésével lehetővé teszi az informatikai rendszerek jogosultságon alapuló használatát.

hitelesítés: a felhasználó személyazonosság ellenőrzésének folyamata. A hitelesítési folyamat egy publikus információ (felhasználói azonosító) és egy privát információ (pl.: jelszó, amit csak a felhasználó ismer; vagy hardver

token, amit a felhasználó birtokol; vagy a felhasználóra jellemző biometrikus azonosító pl. ujjlenyomat) alapján dönti el az érvényességet úgy, hogy összehasonlítja azzal, amit a rendszer ismer.

jogosultság: az arra felhatalmazott személy által adott hozzáférési lehetőség az informatikai rendszerhez/rendszerelemekhez, a különböző jogosultsággal felruházott felhasználók különböző szinten használhatják a rendszer funkcióit.

adatállomány: egy nyilvántartásban kezelt adatok összessége.

adatbázis: azonos jellemzőjű, strukturált adatok összessége, amelyet egy tárolására, lekérdezésére és szerkesztésére alkalmas szoftver kezel.

adatbáziskezelő: az adatbázisban tárolt adatokhoz való hozzáférést biztosító szoftver.

adathordozó: informatikai eszközzel írható vagy olvasható, adatok tárolására alkalmas tárgy (pl.: CD, DVD, szalagos adatkazetta), vagy adatok tárolására szolgáló informatikai eszköz (pl.: pendrive, külső merevlemez).

biztonsági mentés, mentés: biztonsági másolat készítése az informatikai rendszerben tárolt adatokról, illetve a használt szoftverekről. A másolat célja az elsődleges adattároló eszköz megsérülése esetén az adatok helyreállíthatóságának biztosítása.

archiválás: a ritkán használt vagy használaton kívüli, meghaladottá vált, de nem selejtezhető adatok, szoftverek változatlan tartalmi formában történő adathordozóra másolása hosszú távú megőrzés céljából és törlése az elsődleges adattároló eszközről.

eseménynapló, napló: az informatikai rendszerben bekövetkező eseményeket, felhasználói tevékenységeket és ezek időpontját rögzítő, a rendszer által automatikusan kezelt adatállomány, amely a változások észlelését és a számon kérhetőséget biztosítja.

naplózás: az informatikai rendszerben bekövetkező események, felhasználói tevékenységek és ezek időpontjának automatikus rögzítése.

kriptográfia: mindazoknak az eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek az információk illetéktelenek előli elrejtését hivatottak megvalósítani.

titkosítás, rejtjelezés: nyílt üzenetet kódolása kriptográfiai eljárással vagy eszközzel. A rejtjelezés eredménye a titkosított üzenet.

titkosító kulcs: a titkosításhoz és a titkosított üzenetek megfejtéséhez használt szimbólumsorozat.

nyilvános kulcsú titkosítás: olyan kriptográfiai rendszer, amelyben a résztvevők két kulcsot egy közös algoritmussal használnak titkosításra és a titkosított adatok megfejtésére, vagy az adatok hitelesítésére (digitális aláírás) és annak ellenőrzésére. A kulcsok egyikét nevükkel együtt nyilvánosságra hozzák (nyilvános kulcs), a másikat titokban tartják (magánkulcs). Az üzenetet küldő a címzett nyilvános kulcsával titkosítja, a saját magánkulcsával hitelesíti az üzenetet, a címzett csak a saját magánkulcsával tudja megfejteni a titkosított üzenetet, illetve az aláírt üzenet sértetlenségét (és hitelességét) a küldő nyilvános kulcsával ellenőrizheti.

tanúsítvány: olyan bitsorozat, amely valakinek a megnevezését és a nyilvános kulcsát tartalmazza, és amelyet egy megbízható fél (hitelesítés szolgáltató) írt alá.

hitelesítés szolgáltató: olyan mindenki által megbízhatónak tartott, erre szakosodott szervezet, amely tanúsítványokat adhat ki kliensek és szerverek számára.

Alkalmazott megnevezések, rövidítések

A jelen szabályzatban alkalmazott megnevezések és rövidítések a következők:

IBSZ: Informatikai Biztonsági Szabályzat, jelen szabályzat.

Ibtv.: 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

Infotv.: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

Szjt: 1999. évi LXXVI. törvény a szerzői jogról.

technológiai végrehajtási rendelet: 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.

Szervezet: III. kerület Óbuda Békásmegyer Költségvetési Szerveket Kiszolgáló Intézmény (KSZKI)

Üzemeltető: a NetworKing IT Kft., az informatikai rendszerek üzemeltetője.

IT csoport: a KSZKI belső informatikai csoportja

Beszerző szervezet: a beszerzéseket lebonyolító szervezet/szervezeti egység

KSZKI Munkaügyi csoport: a humánerőforrás gazdálkodásért felelős szervezet/szervezeti egysége.

Intézményvezető: a KSZKI intézményvezetője.

informatikai vezető: az IT csoport vezetője

információbiztonsági felelős (IBF): az Ibtv.-nek megfelelően az elektronikus információs rendszerek biztonságáért felelős személy.

rendszergazda: az informatikai rendszer felett a NetworKing IT kft, mint üzemeltető részéről felügyeletet gyakorló személy (külső rendszergazda), illetve az IT csoport, mint belső IT üzemeltetés részéről felügyeletet gyakorló személy (belső rendszergazda).

adatgazdai terület: az a szervezeti egység, amelyhez az informatikai rendszerben tárolt adatok kezelése rendelhető, illetve ahol az adat keletkezik.

kulcsfelhasználó: az informatikai rendszerhez az adatgazdai terület részéről kijelölt, a rendszerben tárolt adatok védelméért, a rendszer funkcionális működéséért felelős felhasználó.

beépített rendszergazdai fiók: a szoftverek és hardver eszközök kiemelt jogosultságú, gyárilag beépített rendszergazdai fiókja (pl.: admin, administrator, root, superuser, sa, stb.), amelyek segítségével a rendszerelem felügyelhető, adminisztrálható.

technikai felhasználói fiók: nem személyhez, hanem szoftverhez, szolgáltatáshoz vagy hardver eszközhöz kötődő felhasználói fiók, amelyet belsőleg használnak valamely más rendszer szolgáltatásának eléréséhez (pl.: egy alkalmazói szoftver használja adatok tárolásához az adatbáziskezelő szerveren; vagy egy multifunkciós nyomtató szkennelt dokumentumok e-mail-ben történő küldéséhez; stb.).

informatikai rendszer: az Ibtv. szerinti elektronikus információs rendszer, amely magában foglalja a hardver eszközöket, a szoftvereket, a hálózati és környezeti infrastruktúra elemeit, valamint tágabb értelemben a szoftverekben kezelt adatokat, az adathordozókat, a dokumentációkat, szabályzatokat és a rendszert kezelő személyeket.

informatikai erőforrások: az informatikai rendszer hardver, szoftver, hálózati és környezeti infrastruktúra elemeinek összessége.

alkalmazói rendszer: a Szervezet tevékenységét közvetlenül támogató informatikai rendszer (pl.: pénzügyi-számviteli rendszer, anyagrendszer, iktatórendszer stb.).

alaprendszer: az alkalmazói szoftverek működéséhez szükséges alap informatikai szolgáltatásokat megvalósító informatikai rendszerek (pl.: központi címtár, fájl szerver szolgáltatások, levelező rendszer stb.).

Helpdesk: a NetworKing IT Kft. által üzemeltetett informatikai rendszer, amely célja a felhasználói oldalon jelentkező, informatikai rendszerekkel kapcsolatos bejelentések fogadása és a bejelentések kezelése.

informatikai eszköz: számítógép, számítógéphez kapcsolódó periféria (pl.: monitor, billentyűzet, egér, nyomtató, szkenner, pendrive, külső merevlemez stb.) vagy egyéb olyan hardver eszköz (pl. hálózati eszköz), amely az informatikai rendszer működéséhez szükséges.

informatikai azonosító: az informatikai eszközhöz a Szervezetnél alkalmazott egységes névkonvenció szerint rendelt egyedi azonosító.

munkaállomás: olyan személyi számítógép (PC), amelyet a felhasználó a napi munkája során használ, és amellyel igénybe veheti a szerverek szolgáltatásait. Lehet asztali számítógép (desktop PC) és hordozható számítógép (laptop, notebook).

mobil eszköz: hordozható számítógép (laptop, notebook) vagy egyéb informatikai és kommunikációs feladatok ellátására használható, operációs rendszerrel, kommunikációs szolgáltatásokkal rendelkező, hordozható eszköz (pl.: mobiltelefon, PDA, táblagép).

mobil adathordozó: informatikai eszköznek minősülő, cserélhető adathordozó (pl.: pendrive, külső merevlemez).

hálózati nyomtató: közvetlenül a hálózatra kapcsolódó nyomtató vagy multifunkciós (fénymásolásra és szkennelésre is alkalmas) nyomtató.

védett terület: az informatikai eszközöket koncentráltan tartalmazó helyiségek (pl.: szerverterem, hálózati rendező helyiség), vagy bizalmas iratokat tartalmazó helyiségek (pl. irattár), illetve a nem védett területnek számító helyiségben elhelyezett egyedi hálózati rack szekrények.

licencköteles szoftver: olyan szoftver, amely használata használati engedélyhez (szoftverlicenchez) kötött, és amelyért a szoftver szerzője használati díjat kér. Ide tartoznak a vásárolt, bérelt vagy belsőleg fejlesztett, illetve külső fejlesztő cég bevonásával fejlesztett szoftverek.

szabad szoftver: olyan szoftver, amelynek licencszerződéséből kétséget kizáróan megállapítható, hogy a szerző vagyoni jogairól lemond, a szoftver használatáért díjat nem kér (freeware szoftverek), illetve bizonyos korlátozásokkal engedélyezi a szoftver használatát díj fizetése nélkül (shareware vagy demo szoftverek).

legális szoftver, jogtiszta szoftver: érvényes használati engedéllyel (szoftverlicenccel) rendelkező, a licencszerződésnek megfelelően használt szoftver. A vásárolt, bérelt, illetve külső fejlesztésű szoftverek esetében a számla, felhasználói licencszerződés/licencigazolás és az eredeti telepítő adathordozók együttes vagy részbeni meglétével kell hitelt érdemlően bizonyítani a használat jogosságát (számlának minden esetben lennie kell). A belső fejlesztésű szoftverek esetén a szoftverlicenc igazolásához a forrásprogram megléte szükséges.

illegális szoftver: érvényes használati engedély (szoftverlicenc) nélkül, vagy nem a licencszerződésnek megfelelően használt szoftver.

vírusvédelmi szoftver: a vírusok és egyéb kártevők (pl.: férgek, kémprogramok, trójai programok) elleni védekezésre szolgáló program, amely képes felismerni, és a legtöbb esetben eltávolítani a fertőzött számítógépről a kártékony programokat.

belső fejlesztés: az Informatika csoport által történő szoftverfejlesztés.

külső fejlesztés: az Informatika csoporton kívül egyéb, külső fejlesztő cég bevonásával történő szoftverfejlesztés.

kiemelt kódrendszer: informatikai rendszerben alkalmazott kiemelt jelentőségű kódrendszer, amelyeket több informatikai rendszer közösen használ és kapcsolódási pontot jelent az egyes informatikai rendszerek között.

központi címtár: a hálózati rendszer felhasználóinak adatait tároló központi adatbázis.

hálózati megosztás: a szerveren elhelyezkedő, programokat vagy dokumentumokat tartalmazó fájl mappa, amelyhez a felhasználók jogosultságokkal szabályozható módon hozzáférhetnek.

Home mappa: a felhasználók saját használatú fájljai, dokumentumai, felhasználóhoz kötődő beállításai, lekérdezései tárolására a felhasználók rendelkezésére bocsájtott, mások által nem elérhető mappa.

távoli hozzáférés: minden olyan hozzáférés a Szervezet informatikai rendszeréhez (felhasználó vagy másik informatikai rendszer által), amelyben a kommunikáció egy külső, nem a Szervezet által ellenőrzött hálózaton (pl. Interneten) zajlik.

SZOFTVERHASZNÁLATI POLITIKA

A szerzői jog által védett szoftverek illegális használata és másolása törvénybe ütköző cselekedet, büntetőjogi felelősségre vonással jár, ellenkezik a Szervezet elveivel. Az ilyen jellegű szoftvermásolást helytelenítjük és elítéljük, ezért ennek megakadályozására a Szervezet a következő alapelveket fogadja el:

- Semmilyen körülmények között nem ösztönzi, és nem tűri el illegális szoftvermásolatok készítését vagy használatát.
- Minden indokolt szoftverigény kielégítésére a Szervezet jogtiszta szoftvert biztosít az összes számítógépre, a megfelelő időben és a szükséges mennyiségben.
- Eleget tesz minden olyan licenc vagy vásárlási feltételnek, törvényi előírásnak, amely az általunk beszerzett vagy használt szoftverek felhasználását szabályozza.
- Az illegális szoftvermásolatok készítésének vagy használatának megakadályozása érdekében belső ellenőrzést végez, beleértve a fenti normák betartatására, és a normákat megszegők fegyelmi büntetésre vonatkozó intézkedéseket.

Az Szervezet számos szoftvercég termékeit használja. A Szervezet szoftverhasználati politikája és rendje előírja, hogy az alkalmazottak tiszteletben tartsák a szoftverekkel kapcsolatos szellemi tulajdonjogot, valamint a használt szoftverek licencszerződéseinek feltételeit. A licencszelt szoftver eszközökkel való gazdálkodás megköveteli, hogy a Szervezet csak jogtiszta szoftvereket telepítsen a számítógépeire, beleértve a hordozható számítógépeket és szervereket is.

A Szervezet minden szükséges lépést megtesz, hogy megakadályozza a licencszelt szoftverek és a kísérő dokumentációk jogsértő másolását, mind a saját telephelyén, mind máshol, kivéve azt az esetet, ha a másolásra a licenctulajdonostól írásbeli engedélyt kapott. A szoftverek engedély nélküli másolása a Szerzői Jogi törvény szerint bűntettnek minősül.

A Szervezet nem adhat engedélyt egyetlen alkalmazottnak sem a szoftverek vonatkozó licencszerződését megsértő használatára, beleértve a szoftverek átadását vagy elfogadását üzleti partnerektől, megbízóktól vagy ügyfelektől.

A Szervezet a szoftverhasználattal kapcsolatosan tájékoztatást nyújt az alkalmazottaknak. Ha az alkalmazottainak tudomására jut, hogy a megvásárolt szoftvert, vagy azzal kapcsolatos dokumentációt nem a fentiek szerint használják, akkor azt kötelesek jelenteni munkáltatójuknak.

A BTK 329/a paragrafusa értelmében az illegális szoftvermásolásban résztvevő személy a megfelelő összeg erejéig kártérítésre kötelezhető. és a törvény értelmében pénzbírsággal is sújtható.

FELHASZNÁLÓI IGÉNYLŐLAP

Név:

….....

Tel:

….....

Szervezeti egység:

….....

Beosztás:

….....

Bejelentkezési azonosító
(rendszergazda tölti ki) ….....

Alapértelmezett jelszó:
(rendszergazda tölti ki) ….....

E-mail cím:
(rendszergazda tölti ki) ….....

A szabályzatban foglaltakat megismertem és magamra nézve kötelezőnek ismerem el.

……

felhasználó aláírása

Dátum:

A felhasználó létrehozását engedélyezem / nem engedélyezem.

…….

ELFOGADÓ NYILATKOZAT

Név	Aláírás	Dátum
Novák Zsolt		
Baranyai Krisztina		
Bakonyi Rita		
Bécsi Krisztina		
Beséné Gold Anna		
Beszta Adrienn		
Bodrogi Orsolya		
Borbás Pálma		
Cserkuti Erika		
Csóti Anita		
Domokosné Zubó Katalin Viktória		
Dömötör Lívia		
Dr. Lévai-Bagoly Ildikó		
Forgács Rita		
Gellén József		
Gulya Ágnes		
Hausknecht Józsefné		
Hoffer Kovács Beáta		
Illés Orsolya		
Könyves Jánosné		

Név	Aláírás	Dátum
Kulcsár Katalin		
Kocsordiné Tóth Erzsébet		
Laskai Szabina		
Márkus Ildikó		
Mikó Attila		
Moldvai Tímea		
Sidlovszky Viktória		
Simányi Péter		
Szikora Pál		
Szikora Krisztiánné		
Szőgyéni Péter		
Szőke Éva		
Tóthné Borbély Rozália		
Ujvári Krisztina		
Vérné Monostori Viktória		