FŐK/1791-099/23.

SZ82

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

VÁCI JÁVORSZKY ÖDÖN KÓRHÁZ					
Dokumentum cím		Informatikai biztonsági szabályzat		**Azonosító**	SZ82
Verziószám	3	**Jóváhagyás dátuma**	2023.09.08	**Oldalak száma**	58
Készítette		Schulmann Péter, informatikai biztonsági felelős			
Ellenőrizte		Boda Péter informatikai osztályvezető			
Minőségügyi szempontból ellenőrizte		Vass Csilla mb. minőségügyi vezető			
Jóváhagyta		Dr. Urbán Edina főigazgató főorvos			

IT SCHecurity Kft.
2800 Tatabánya, Jegenye utca 40.
Adószám: 29034842-2-11
EU Tax Num.: HU29034842
Erste Bank: 11600006-00000000-94798696

Módosítás		
Hatályba lépés dátuma	**Verziószáma**	**Helye a szabályozásban**
2018.05.24.	1	Új szabályozó dokumentum
2022.10.11.	2	Teljesen átdolgozott kiadás
2023.09.11.	3	3.1.1.1.2.1.2., 3.1.1.1.2.3., 3.1.1.1.2.4.

Tartalom

3.1.1.1.1. Az érintett szervezet

A Váci Váci Jávorszky Ödön Kórház (2600 Vác, Argenti Döme tér 1-3.) Informatikai Biztonsági Szabályzata.

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

3.1.1.1.1.3. Jogosultságok

Jelen szabályozás a Váci Jávorszky Ödön Kórház és Szakrendelő tulajdona, tartalmának megismerésére, csak a Váci Jávorszky Ödön Kórház és Szakrendelő 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

Az alapfogalmakat jelen szabályzat 4.1 melléklete tartalmazza

3.1.1.1.2.1.1.Célok

Az Informatikai Szabályzat elsődleges célja a Váci Jávorszky Ödön Kórház és Szakrendelő informatikai rendszereinek a jogszabályoknak megfelelő biztonságos és áttekinthető működtetése, illetve a számítástechnikai eszközök beszerzésének informatikai biztonsági szempontból történő szabályozása. A vállalaton 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 számon kérhető a biztonsági intézkedések működtetése, alkalmazása.
Határozza meg az IT Biztonsági intézkedés végrehajtásában, alkalmazásában közreműködő egyéb szereplőket, érintetteit és azok feladatait.
Az IT Biztonsági Szabályzatban meghatározott biztonsági intézkedések részletes végrehajtási utasításait, eljárásait kapcsolódó dokumentumok, mint például üzemeltetési kézikönyvek, felhasználói kézikönyvek tartalmazzák.
Jelen dokumentum a vállalat 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 vállalat minden alrendszerére érvényes informatikai biztonsági szabályokat.

3.1.1.1.2.1.2. A számítástechnikai rendszerek üzemeltetésének, fenntartásának célja

Az Intézménynél 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. *Magáncélú használat engedélyezése esetén az eszközön a magáncélú tartalmakat egyértelműen megjelölve és elkülönítve kell tárolni, abba csak alapos gyanú esetén lehet betekinteni.*

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
- Mentési szabályzat
- Hozzáférés-kezelési szabályzat (Integrált)
- Eljárásrendek (Integrált)
- Biztonsági Osztályba sorolás (Integrált)
- Kockázatelemzés (Integrált)
- Adatvédelmi és adatbiztonsági szabályzat

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

3.1.1.1.2.1.4. A Szabályzat tárgyi és személyi hatálya

A Szabályzat hatálya kiterjed — az érintettek körén keresztül — Az Intézmény tulajdonában lévő összes számítástechnikai eszköz használatára (tárgyi hatály).
Az érintettek körének meghatározása (személyi hatály):

- A Váci Jávorszky Ödön Kórház és Szakrendelő vezető beosztású dolgozói (Főigazgató és helyettese, Igazgatók, Osztályvezetők, Munkáltatói joggyakorlók)
- Számítógépet használó alkalmazottak, megbízottak, felhasználók
- Rendszergazdák
- Külső munkatársak (szerződéses, és egyéb megbízással)
- Bármely felhasználó által engedélyezett, jogviszony nélküli „vendég"

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
- 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
  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 az Intézmény 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 licence-ekről nyilvántartást kell vezetni. A licence nyilvántartás kérdése hozzákapcsolódik más IT eszközök nyilvántartásához. A licence-ek nyilvántartása az IT üzemeltetés, a nyilvántartás értékelése az IT biztonságért felelős vezető feladata. Amennyiben licence-igény következik be, az IT biztonságért felelős vezető tesz javaslatot a probléma feloldására.
Az általános Adatvédelmi Rendelet (GDPR) 30. cikke szerinti adatkezelési nyilvántartást el kell készíteni és folyamatosan naprakészen kell tartani. A nyilvántartások elkészítése és karbantartása az adatvédelmi tisztviselő (DPO) felelőssége. A nyilvántartás elkészítéséhez az Adatgazdáknak információt kell nyújtaniuk.

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 felhasználásra, kizárólag vezetői engedély alapján mentesülhet ez alól. Magáncélú használat engedélyezése esetén az eszközön a magáncélú tartalmakat egyértelműen megjelölve és elkülönítve kell tárolni, abba csak alapos gyanú esetén lehet betekinteni.
A felhasználó köteles e dokumentumban leírt szabályokat betartani. E dokumentumtól egyéni megegyezés keretében el lehet térni. Az eltérést jóvá kell hagynia az Informatikai osztálynak, vagy az Igazgatóságnak.
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 Az Intézmény szoftvereit magáncélra lemásolni, sem más gépre telepíteni.
A felhasználó Az Intézmény 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
Az Intézmény a saját levelezőrendszerét használja.
A központi, vállalati levelezőrendszer kizárólagos célja a munkavégzés. A felhasználó nem jogosult magáncélra használni a levelezőrendszert.
Az Intézmény 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 vállalat 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.

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
A kockázatelemzés készítésének módszertani leiratának rövidített példánya.

Kockázatelemzési módszertani leírat – rövidített (lásd még 4.2 melléklet)

A felmérés
Az ellenőrzés tervezése során az első lépések egyike a környezet értelmezése, megismerése, amelyben a szervezet működik. Ennek alapján azonosíthatók és kategorizálhatók azok a kockázatok, amelyek meghatározzák az ellenőrzés lefolytatását. Az ellenőrzési kockázat összetevői a belső (inherens) kockázat, az ellenőrzési mechanizmusból eredő kockázat, az észlelési kockázat. A belső (inherens) kockázat olyan hiba előfordulásának kockázata, amelyre nincs helyettesítő ellenőrzési eljárás. Az ellenőrzési mechanizmusból eredő kockázat annak a kockázata, hogy a belső ellenőrzési eljárások során nem feltárt, vagy nem megelőzött hibák, hiányosságok maradnak. Az észlelési kockázat annak a kockázata, hogy az ellenőr nem megfelelő teszteljárást alkalmaz az ellenőrzés során, és így figyelmen kívül hagy lényeges hiányosságokat, hibákat. Az ellenőrizendő területek meghatározása előtti kockázatfelmérés indokai:

- Támogatja a menedzsmentet a források hatékony allokálásában,
- Segíti az ellenőrzési célok beillesztését az üzleti tervekbe, megfeleltcti azokat a szervezeti céloknak,
- Megalapozza a belső ellenőrzési tevékenység menedzsmentjét,
- Megbízható információkkal szolgál a magas üzleti kockázatú területekről

A kockázatra koncentráló ellenőrzés lépései:

- Információk gyűjtése,
- Belső ellenőrzési eljárások megértése,
- Ellenőrzés lezárása.

Az információgyűjtés célja, hogy az ellenőr a vizsgálandó kontroll eljárásról, annak üzleti és szervezeti környezetéről minél többet tudjon meg. Így azonosításra kerülnek az érintett egyének, folyamatok, helyszínek, és azok az eljárások, amelyek érintettek a kontroll mechanizmusban. A lehetséges témakörök:

- üzleti elvárások és a kapcsolódó kockázat,
- szervezeti struktúra,
- feladatok és felelősök,
- vállalati (intézményi) politika és eljárások,
- jogok és szabályok,
- kontroll eszközök,
- riportok,
- érintett informatikai erőforrások.

Az ellenőrzés nagyon fontos része a részletes dokumentálás, ami biztosítja a teljes megértést és a további munka gördülékenységét. Fontosak az alábbi (szinte minden esetben) megválaszolandó kérdések:

- ki végzi a feladatot,
- hol végzi,
- mikor végzi,
- melyek a feladathoz szükséges inputok,
- mely outputokat kell szolgáltatnia a feladatnak
- hogyan történik a megvalósítás az elképzelések szerint.

A beviteli kontroll eljárások során az ellenőr értékeli az észlelési kockázatot, vizsgálja az kontroll eljárások környezetét, magát az eljárást, felméri a kontroll mechanizmusból eredő kockázatot.
A kontroll mechanizmusok kipróbálását a lényegi (szubsztantív) teszt követi.
Az ellenőrzés lezárása az ellenőrzési jelentés elkészítését jelenti, a javaslatok megfogalmazásával együtt, amelyet az ellenőrzött terület vezetőjével egyeztetni szükséges.

Menedzsment politikák, ellenőrzés és kockázatok

A rendszer legfontosabb eleme az ember. Itt nem csak az intézmény dolgozóira kell gondolni, hanem mindazokra, akik valamilyen, akár részmunkaidős foglalkoztatás keretében, akár külső szolgáltatás keretében a rendszer részeivé válnak.

Külföldi és a hazai szakirodalom azt a tényt támasztja alá, hogy az emberi tényező a legnagyobb kockázati tényező a rendszerben. Ez azt jelenti, hogy a humánerőforrás kezelés nem elhanyagolható kérdése a biztonságos és megbízható működésnek.
Az emberi hibák lehetnek a hozzá nem értésből származó, jó szándékú és szándékosan elkövetett károkozás, cselekmények.
Számos esetben bizonyos fokú védelmet jelent az oktatás, az adott munkakörhöz szükséges képesítés megszerzése.
Az egyik legnagyobb veszély a személyzet, a dolgozók által ismert bizalmas információk nyilvánosságra hozatala. A statisztikák azt mutatják, hogy egy szervezet adatainak bizalmasságát, hitelességét és sérthetetlenségét az esetek 80%-ban a szervezet munkatársai sértik meg, saját vagy külső motiváció hatására, illetve saját hibájukból.
Szándékos károkozást válthat ki például valamilyen konfliktushelyzet a vállalati szereplők között (például fegyelmi eljárás, elbocsátás). Kockázati tényezőt jelenthetnek a káros szenvedélyekkel bíró dolgozók (például kábítószer, szerencsejátékok, túlzott költekezés), akiknél igen nagy esély van a pénzszerzési kényszerből elkövetett károkozásnak. A számítógépes bűnözés gyakran irányul a vagyonszerzésre, a vállalatoknál található értékek megszerzésére. Kiemelkedő helyet foglal el a pénz és a titkok megszerzésére irányuló tevékenység. Ebbe a csoportba tartozik a rablás, csalás, zsarolás, lopás, megvesztegetés, valamint a túszszedés és a terrorizmus is.
A személyek által okozott adat- és információvesztés okai a következők lehetnek:

- Munkafolyamatok speciális jellegéből adódó veszélyforrások;
- Gondatlanul okozott események (például e-mail téves helyre küldése);
- Személyes vagy munkahelyi túlterhelés (például stressz vagy családi problémák);
- Előírások, szabályok ismeretének hiánya;
- Előírások, szabályok nem megfelelősége, munkamenet hibás szabályozása;
- Előírások, munkaköri leírások figyelmen kívül hagyása;
- Hiányos biztonságtudat (nem ismerik fel a valós veszélyeket);
- Túlkomplikált kezelés (a bonyolultsággal arányosan nő a hiba elkövetésének valószínűsége);
- Hiányzó ellenőrzés;
- Szándékos cselekmények.

Az angol nyelvű szakirodalom 7-E néven említi az informatikai biztonságot fenyegető legfontosabb tényezőket. Ezek az alábbiak:

1. személyiség (ego),
2. lehallgatás (eavesdropping),
3. ellenségeskedés (enmity),
4. kémkedés (espionage),
5. sikkasztás (enbezzlement),
6. zsarolás (extortion),
7. hiba (error).

A felsorolásból is világos, hogy a legnagyobb problémát az emberi tényező okozza, hiszen a hét tényező mindegyikének köze van hozzá. Így tehát az informatikai biztonság hatékonyságát nagyban befolyásolja a humán oldalra történő koncentrálás.

A kockázat meghatározása

A kockázat

A kockázat matematikai definíció szerint a kár várható értéke egy adott időszakban.

Képletben:

$R = \sum p(t)d(t)$,

Ahol ***R*** a kockázat (risk), ***T*** a veszélyforrások halmaza (threat), ***pt*** egy adott veszélyforrás bekövetkezési valószínűsége (probability), ***dt*** pedig a keletkező kár (damage) mértéke

Kockázati paraméterek becslése

Egy informatikai rendszer esetében azért van különösen nehéz feladatunk a kockázat mértékének pontos meghatározásakor, mert a fenti képlet egyetlen paraméterét sem tudjuk jól megbecsülni. A veszélyforrások listája sem lehet teljes; sok esetben a bekövetkezési valószínűség becsléséhez nem áll rendelkezésre korábbi statisztikai, tapasztalati érték; a keletkezett kár pedig egy informatikai rendszerben komplex, áttételes hatásmechanizmuson keresztül realizálódik, amely hatásmechanizmus feltérképezése, és a kár pénzben kifejezett meghatározása sem magától értetődő.
Informatikai rendszerek esetén a veszélyforrások általában konkrét rendszerelemeket támadnak, majd az egyes rendszerelemek sérülése hat a velük kapcsolatban lévő alkalmazásokra, amelyeken keresztül a munkafolyamatokban – mind az alaptevékenységben, mind az operatív, taktikai és stratégiai irányításban is – fennakadások lehetnek. Amennyiben a kár hatását nem sikerül jól kezelni, a fennakadás az ügyfelek, partnerek, üzleti folyamatok szintjén is érzékelhető lehet és ez szélsőséges esetben piaci hatásokhoz is vezethet (imázs romlás, ügyfelek elpártolása, piacvesztés). A hatás továbbterjedésének megfelelően szokás ezért úgynevezett *elsődleges, másodlagos, harmadlagos* stb. kárról beszélni.
Egy informatikai rendszer esetében a másodlagos, harmadlagos károk nagyságrendekkel nagyobbak az elsődleges, károknál, ezért rendkívül fontos minden veszélyforrás esetén egyenként elbírálni, hogy az esetlegesen bekövetkező hatás meddig terjedhet ki.
Például egy egyszerű merevlemez meghibásodása okozhatja, hogy nagy mennyiségű adat visszaállíthatatlanul megsemmisül. Ilyenkor az elsődleges kár, a merevlemez megjavításának költsége eltörpül az áttételesen okozott károkhoz viszonyulva. Az elveszett adatok pótlásának költségei, a visszaállítás ideje alatt fennakadt üzleti folyamatok és még rosszabb esetben az ennek hatására elmaradt üzleti haszon hatalmasak lehetnek a bekövetkezés konkrét okától függetlenül.
Tekintve, hogy informatikai rendszerekben a veszélyek, károk, illetve kockázati tényezők hatásmechanizmusa ennyire összetett, gyakorlatilag egyetlen komoly módszertan sem vállalkozik arra, hogy a kockázat pénzügyi nagyságát közvetlenül megbecsülje, forintosítsa.

Kockázatelemzés, kockázatmenedzsment

A legtöbb, gyakorlatban alkalmazott kockázatbecslési módszertan a kategorizálás módszerét alkalmazza, azaz csak nagy nagyságrendben határozza meg a bekövetkezés valószínűségét és a kár nagyságát. Ez ugyan nem teszi lehetővé, hogy a biztosításokhoz hasonlóan, számszerű

kockázati értéket határozzunk meg egy veszélyforráshoz, de már jó kiinduló pontot ad. Az *egyes kockázati tényezőket egymáshoz hasonlítva* határozzuk meg a gyenge láncszemeket, azokat a pontokat, ahol a legcélszerűbb védekezni. Ezt a folyamatot nevezzük kockázatelemzésnek vagy kockázatmenedzselésnek, nevében is megkülönböztetve a kockázatbecsléstől.

A kockázatelemzés táblázatos módszere

A kockázatok menedzselésének gyakorlati kivitelezésére számos eltérő módszertan létezik. Az alábbiakban egy leegyszerűsített táblázatos módszert mutatunk be, amely ilyen formában nem teljes, de a folyamatot kellően jól reprezentálja.
A módszer alapja a veszélyforrások számbavétele és részletes elemzése, mely az alábbi kockázatelemzési tábla szisztematikus, oszlopról-oszlopra haladó kitöltésével történik.

ID	Veszélyforrás	Bekövetkezés valószínűsége	Kár			Kockázat	Védelmi intézkedés
			C	I	A	R	
Szl	1. szervezeti veszélyforrás						
Sz2	2. szervezeti vf.						
Tl	1. természeti vf.						
Hl	1. humán vf.						
Ll	1. logikai vf.						
Fl	1. fizikai vf.						

Kockázatelemzési tábla szisztematikus, oszlopról-oszlopra haladó kitöltésével történik.

A kockázatelemzés lépései:

1. lépés: Kategóriák felállítása
   - Bekövetkezési valószínűség kategóriái
   - Kár kategóriák
   - Kockázati kategóriák
   - Kockázati szorzótábla meghatározása
2. lépés: Veszélyforrások listájának összeállítása
3. lépés: Bekövetkezési valószínűségek nagyságrendi becslése
4. lépés: Kárértékek nagyságrendi meghatározása
5. lépés: Kockázati tényezők származtatása
6. lépés: Elviselhetetlen kockázatok kezelése
7. lépés: Lehetséges védelmi intézkedések számbavétele és a megfelelő alternatívák kiválasztása

A lépéseket végrehajtva az előállított kitöltött tábla hatékony eszköz biztonsági szempontból gyengén védett területek felismeréséhez, megfelelő kezeléséhez, biztonsági kérdések menedzsmentjéhez, illetve végső soron a megfelelő, egyenszilárdságú védelmet nyújtó intézkedések meghatározásához.

Kockázat kezelésének módszerei

A kockázatelemzés eredményeként képet kapunk egy rendszert fenyegető veszélyforrásokról, a bekövetkezési valószínűségeken és becsült kár értékeken keresztül pedig a fellépő kockázat egymáshoz viszonyított nagyságáról. A kockázatmenedzsment célja ennek ismeretében a kockázat hatékony csökkentése, ezáltal a biztonság növelése.
Egy kockázati tényező kezelésére alapvetően három eszköz áll rendelkezésünkre:

- a kockázat csökkentése megfelelő szintű védekezéssel,
- a kockázat áthárítása,
- tudatos kockázatvállalás.

Védekezés

A kockázatot a bekövetkezési valószínűségek és az okozott károk szorzatainak összegeként definiáljuk, így csökkentése e tényezők csökkentésével valósulhat meg. A kockázatcsökkentés alapmódszerei tehát:

- a bekövetkezési valószínűség csökkentése,
- a veszélyforrás kiküszöbölése,
- az okozott kár nagyságának korlátozása, csökkentése.

A megfelelő szintű védekezési módszerek tervezésére általánosan elfogadott és a gyakorlatban is rendkívül jól alkalmazható szemlélet az úgy nevezett PreDeCo kontrollok rendszere alkalmazható. A név a három fő mechanizmus angol nevének kezdetéből áll:
Preventive: megelőző, kivédő kontrollok
Detective: felismerő kontrollok
Corrective: elhárító, helyreállító kontrollok
A PreDeCo szemlélet szerint egy kontroll cél (control objective) biztosítására tett védelmi intézkedések e három, alapvetően más működésű védelmi mechanizmus ötvözéséből tevődnek össze:
A *bekövetkezési valószínűség csökkenthető* erősebb védelmi mechanizmus (megelőző intézkedések) alkalmazásával.
A *veszélyforrások kiküszöbölése* tulajdonképpen tekinthető a bekövetkezési valószínűség csökkentés speciális esetének is, azzal a lényeges kitétellel, hogy ez a valószínűség itt közel nullára csökken. Sajnos a veszélyforrások kiküszöbölése védekezéssel általában nem valósítható meg. Bizonyos ritka esetekben nyílik csak erre lehetőség (pl. megfelelő villámvédelemmel a villámcsapás hatása gyakorlatilag kivédhető). A teljes kiküszöbölés a legtöbb esetben csak megfelelő *architekturális átszervezéssel* oldható meg (új operációs rendszerek telepítésétől a manuális visszaellenőrzésekig), amelyek kivitelezése csak nagyon ritkán jelent reális alternatívát.
A kockázat csökkentésének fontos eszköze a keletkező *kár nagyságának csökkentése.* Általában azonban csak a kár mértékének korlátozásáról beszélünk. A másodlagos, harmadlagos, egyre nagyobb kárt okozó hatásmechanizmust úgy kezelhetjük, ha az elsődleges károknál, illetve a lehető legalacsonyabb szinten „megakadályozzuk" a kár továbbterjedését. Ehhez minél előbb felismerni (detekció) és minél gyorsabban orvosolni (korrekció) kell a problémát. A károk továbbterjedési mechanizmusának feltérképezése után megfelelő átszervezéssel és a megszüntethető függőségek felszámolásával tovább korlátozható a kár terjedése.

A különösen nagy kárt okozó veszélyhelyzetek lekezelésére célszerű külön felkészülni, úgynevezett katasztrófa-elhárítási tervek készítésével, illetve természetszerűleg az ilyen helyzetekre számító felkészülési tevékenységek végzésével (például biztonsági mentések készítésével).

Kockázat-áthárítás

Ha a kár bekövetkezését megakadályozni már nem tudjuk, akkor a kockázat és ezzel a károk áthárítása sok esetben még enyhítheti, orvosolhatja a problémát.
A kockázat-áthárítás elvét követve, például a beszállítókkal, illetve az ügyfelekkel olyan szerződést köthetünk, hogy bizonyos veszélyforrások következményeit ők viseljék. Például bankkártyáknál, ha a PIN-kód illetéktelen kezekbe kerül, akkor a jogosulatlan pénzfelvételért nem a bankot, hanem a kártya birtokosát terhelik az ebből származó veszteségek.
Az áthárítás másik módja *biztosítás* kötése. A biztosítás a bekövetkezett károk pénzügyi kezelését könnyíti. A biztosítási összeggel azonban meg kell fizetni a biztosító kockázatát és költségeit is, így a biztosításként kifizetendő összeg minden esetben meghaladja a kiküszöbölni szándékozott kockázatot. Bár a biztosítás a károk és a kiadások összegének várható értékét nem csökkenti, azaz célszerűtlennek látszik ezt a védelmet alkalmazni, sok esetben mégis érdemes, mert megvédi a céget a kirívóan nagy veszteségektől, amelyek további sokkal nehezebben kezelhető és nagyobb veszteségeket jelentő károkat indukálhatnak. Informatikai kockázatok tekintetében a biztosítási lehetőségek sajnos még elöggé szűkösek.

Tudatos kockázatvállalás

A megfelelő biztonságérzet kialakítása nem más, mint tudatos kockázatvállalás. Mint láttuk, bizonyos veszélyforrások ellen csak célszerűtlenül nagy költségekkel lehet védekezni. Ilyen esetekben a veszélyforrás által jelentett kockázat vállalható, azonban ezen kockázatokkal feltétlenül tisztában kell lenni. A kockázat vállalására irányuló döntést minden esetben a felső vezetésnek kell meghoznia, illetve jóváhagynia.

Lehetséges védelmi intézkedések számbavétele

A védekezési lehetőségeket célszerű külön dokumentumban, táblázatban összegyűjteni. Az egyes lehetőségekhez fel kell mérni a beruházás és az üzemeltetés nagyságrendi költségeit, valamint az általuk kielégített követelményeket. A könnyebb áttekinthetőség, hivatkozhatóság érdekében a védekezési lehetőségekhez hasonlóan a veszélyforrásokhoz azonosító rendelhető. A kockázatelemzési táblázatba ugyanis már csak a javasolt védekezési lehetőségek azonosítói kerülnek.
A kockázatmenedzselés elve szerint a megfelelő védelmi intézkedéseket úgy lenne célszerű kiválasztani, hogy felírjuk az összes elképzelhető védelmi intézkedést, mindegyiknél megadjuk, hogy milyen hatása van, majd az összes lehetséges kombináció értékelésével megkaphatjuk, hogy melyeket kell kiválasztani ahhoz, hogy az összes elviselhetetlen veszélyforrást megfelelően lefedjük, valamint a maradvány kockázat és a védelmi költségek összege a lehető legkisebb legyen. A gyakorlatban azonban egy szakember hozzávetőlegesen meg tudja adni, hogy az adott esetben mely védelmi intézkedések alkalmazása jöhet szóba. Ezen alternatívák közötti választásban nyújt segítséget a kockázatelemzés.
Az egyes védelmi intézkedések közötti választás legfontosabb szempontja az ár és az elért hatás. Költségek tekintetében célszerű megkülönböztetni az egyszeri beruházási költségeket az éves fenntartási költségektől. Egy adott módszer kiválasztásánál a rövid- és hosszú távú pénzügyi célok jól elkülöníthetőek.

A következő táblázat a védelmi intézkedések, azok költségeinek és hatásainak összefoglalására példa:

ID	Védelmi intézkedés	Beruházás	Éves költség	Hatás
V1	Szünetmentes táp	5 000 000	50 000	F1/D, F1/P
V2	Áramfejlesztő aggregátor	10 000 000	200 000	F1/E

A védelmi intézkedések egymásra is hatással vannak, ezért a veszélyforrásokra gyakorolt hatásaikat már nem szokás kategorikusan meghatározni, sőt egyes hatásokat csak informálisan, szóban lehet kellően jól leírni (pl. rejtjelezett levelezés bevezetése megakadályozza a tartalomszűrő tűzfal azon funkcióját, amely levelek mellékleteiből képes a vírusokat kiszűrni).
A veszélyforrásokra gyakorolt hatást egyszerű módon a valószínűség, illetve a hatás csökkentésének mértékével adhatjuk meg.
A hatás leírásában meg kell adni az intézkedés által befolyásolt veszélyforrás azonosítóját, valamint a befolyásolás módját. Ez kiegészíthető még a védelmi intézkedések egymásra hatásának jelölésével.

A hatásmegjelölés magyarázata:
E: (eliminates) a veszélyforás teljes kiküszöbölése
D: (decreases damage) az okozott kár egy kategóriával csökken
DD: (decreases damage) az okozott kár két kategóriával csökken
P: (decrease probability) a bekövetkezési valószínűség egy kategóriával csökken
PP: (decrease probability) a bekövetkezési valószínűség két kategóriával csökken

Több védelmi intézkedés együttes alkalmazása esetén a valószínűségek, illetve kár kategóriák csökkentése nem feltétlenül adódik össze, de a P és D hatás általában összevonható.
A védelmi alternatívák közötti választás algoritmusa általában manuális, vezetői döntést igényel. Sokszor a rövid/hosszú távú, éves költség, avagy beruházás jellegű felsővezetői szintű stratégiai döntések is közre játszhatnak a végső választásban.

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 folytatni, 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 fennállnak-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 védelmi intézkedéseket szükséges bevezetni. 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 min. félévente kötelező megváltoztatni.
A rendszergazdai jogosultsággal rendelkező felhasználók felhasználó nevüket és jelszavukat zárt borítékban kötelesek elhelyezni a Igazgatóság 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 hivatalban 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.

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 (alapszolgáltatások). Az alapszolgáltatási 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 belépő egyedi azonosítóját
- A belépés idejét
- A kilépés idejét
- A használat során módosított adatokat tételesen
- 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. Az Intézmény 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.

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:
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)
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 tarozó 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 Elektronikus Információbiztonsági Hatóság (NEIH) által közzétett és honlapján elérhető „Osztályba Sorolás és Védelmi intézkedés űrlap" specifikációit kell igénybe venni. A besorolási segédlet az IBSZ elektronikus melléklete.

3.1.1.2. Az elektronikus információs rendszerek biztonságáért felelős személy

Az Intézmény 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 a szervezet felsővezetése 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.

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 Informatikai biztonsági felelős a felelős.

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 irányadó.

3.1.1.3.1.2.2. Felülvizsgálat

IIa 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

Az Intézmény informatikai eszközei a következő kategóriákba vannak besorolva.

- Alkalmazások.
- Szoftverek.
- Szerverek.
- Hálózati aktív elemek.
- Hálózatok.
- Felhasználói munkaállomások.
- Nyomtatók, szkennerek.
- 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.

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:
  - Megnevezését
  - Moduljait
  - Alapfeladatát
  - Licenszeit
  - Adatgazdáját/rendszergazdáját
  - Beszállítóját
- A beszállítók:

- Hivatalos nevét
- Adószámát
- Címét
- Telefonszámát
- Mailcímét
- Kapcsolattartóját

- A felelősök:
  - Nevét
  - Munkáltatóját
  - Születési adatait
  - Lakcímét
  - Telefonszámát
  - 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.)
f) 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;
l) 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, Az Intézmény hatókörébe tartozó rendszerre.

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 megszüntetését, 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.

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 kockázatok felmérése az Kockázatkezelési eljárásrend kiegészítő szabályzatban kerül kifejtésre.

3.1.2.1.2.2. A kockázatok kezelésének felelőssége

A kockázatok kezelésének felelőssége minden esetben a szervezet vezetőjét terheli.

3.1.2.1.2.3. A kockázatok kezelésének elvárt minősége

A kialakított módszertannál, a NEIH által közétett IBMK alapján az alábbi tételeket alkalmaztuk.

- Valamennyi olyan rendszerelemet védeni kell a fenyegetésektől, amelyektől a rendszer működése és egyes alkalmazásai függnek, és amelyeket valamely fenyegetés negatívan érinthet.
- Az egyes elemcsoportok között komplex függőségek állnak fenn: egy rendszerelem bizalmassága, sértetlensége és rendelkezésre állása más rendszerelemek bizalmasságát, sértetlenségét és rendelkezésre állását feltételezi.
- A rendszerelemekhez egyedileg meg kell határozni a fenyegetéseket, amelyek a vizsgált környezetben felléphetnek. Miután nem védekezhetünk ezek mindegyike ellen tökéletesen, meg kell ismernünk a legfontosabbakat. Ehhez az összes feltárt fenyegetést értékelnünk kell. Az értékelés függ a kár bekövetkezésének valószínűségétől és a bekövetkezett kár nagyságától, amennyiben a fenyegetés kifejti hatását. Ebből a két részből tevődik össze a kockázat.
- A bekövetkezés valószínűsége olyan eseményeknél, amelyeket emberek célzottan okoznak, a potenciális tettesek felkutatásával és azok számának megadásával becsülhető meg, akik a megfelelő lehetőségekkel és ismeretekkel rendelkeznek. Az olyan események gyakoriságát, melyek műszaki hibák vagy vis maior esetek által lépnek fel, statisztikák és saját tapasztalatok összegzésével lehet megbecsülni. Ugyanez érvényes a személyek akaratlan hibás tevékenysége miatt bekövetkező károk gyakoriságának becslésére. A statisztikákat a szerint kell figyelembe venni, hogy milyen körülmények között készültek; azokat nem lehet egy az egyben átvenni, és egy adott felhasználó speciális körülményeire alkalmazni. Gondolni kell arra is, hogy a statisztikai adatok mindig tartalmaznak bizonytalanságokat.
- A kárnagyság előzetes értékelésekor mérlegelni kell, hogy az adott fenyegetés hatására milyen anyagi és más természetű károk következnek be, melyek a közvetlen károk, és milyen későbbi következményekkel (úgynevezett következményes károkkal) kell számolni.

3.1.2.2. Biztonsági osztályba sorolás

3.1.2.2.1.1. A Besorolás

Az Intézmény 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 eredménye:

Medikai rendszerek : 3.3.3. (általánosan)

- eMedSolution : 3.3.3.
- Gyurika : 2.3.3.
- Főnix : 3.3.3.

Ügyviteli rendszerek: 2.2.2 (általánosan)

- DMSone Pro : 2.2.2.
- jDolBer : 2.2.2.
- CT-EcoSTAT : 2.2.3.

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 az informatikai biztonsági szabályzatban, és igény esetén 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

Az Intézmény 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.
Az Intézmény 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 értelmezhetőek legyenek.
A fejlesztésekre vonatkozó szerződésekben, ill. a szerződésekhez tarozó 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 Az Intézmény 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

Az Intézmény 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

Az Intézmény gondoskodik 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

Az Intézmény 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

Az Intézmény 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

Az Intézmény meghatározza és dokumentálja a felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban.

3.1.3.6.1.3. Ellenőrzés

Az Intézmény 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

Az Intézmény 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. Korrekció

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

Az Intézmény az ellenőrzések megállapításait legalább évente ismerteti az érintett személyekkel.

3.1.4.1. Üzletmenet-folytonosságra vonatkozó eljárásrend

3.1.4.1.1.1. Kihirdetés

Az Intézmény 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

Az Intézmény az üzletmenet-folytonossági tervet, éves gyakorisággal felülvizsgálja és frissíti.

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

3.1.4.2.1.1. Kihirdetés

Az Intézmény megfogalmazza, és az érvényes követelmények szerint dokumentálja, valamint Az Intézményen 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

Az Intézmény összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével.

3.1.4.2.1.3. Felülvizsgálat

Az Intézmény éves gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet.

3.1.4.2.1.4. Aktualizálás

Az Intézmény 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

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

A dokumentum tartalmát megismerheti

- vezérigazgató
- rendszergazda
- adatgazda
- informatikai osztályvezető
- információbiztonsági felelős
- érintett felhasználó Nyilvántartás szerintiek
- érintett szolgáltató Nyilvántartás szerintiek

3.1.4.2.1.6. Bizalmasság

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

3.1.4.2.1.7. Alapfeladatok meghatározása

Az Intézmény elsődleges feladata egészségügyi szolgáltatás biztosítása, ehhez nélkülözhetetlen rendszerek:

- Ügyviteli rendszerek
- Medikai rendszerek

Az alapszolgáltatási kötelezettségekről külön törvények rendelkeznek, a medikai rendszer tűrőképessége 2 nap, amennyiben ez idő alatt nem áll helyre a rendszer, az Főigazgató elrendeli az alternatív rendszer élesítését. Az alternatív rendszer indításához, a felkészülést az 1 üzemszüneti napon kell megkezdeni.

3.1.4.2.1.8. Helyreállítás

Amennyiben a számlázási rendszer a 2.-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 számlázási rendszer felkészítése (fogadó adatgazda)
- Az adatvédelmi bejelentések elkészítése a fogadó adatfeldolgozói tevékenységéről, és a feladatok elvégzéséhez szükséges szerződések megkötése (Főigazgató – adatvédelmi felelős)
- Az adatok átadása/átvétele (átadó adatgazda – fogadó adatgazda)
- Előzetes tesztelés (fogadó rendszergazda)
- A számlázási rendszer élesítése (átadó rendszergazda – átadó adatgazda)
- A számlázás megkezdése (fogadó adatgazda)

3.1.4.2.1.9. Szerepkörök, felelősségek

Főigazgató – döntéshozatal, kapcsolattartás

Gazdasági igazgató – döntéshozatal, folyamatok értékelése
Rendszergazda – Helyreállítás (Hardver- Szoftver) kapcsolattartás
Adatgazda – Az adatok sértetlenségének, bizalmasságának, rendelkezésre állásának fenntartása.
Informatikai vezető – erőforrások biztosítása
Információbiztonsági felelős - fent tarja az előírások betartását, minden körülmények között, javasol és részt vesz a döntés előkészítésben, dokumentál
Felhasználó – a kapott utasítások végrehajtása

3.1.4.2.1.10. Alapfeladatok biztosítása

Az Intézmény fenntartja a szervezet által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is, ezek:

Ügyviteli rendszer
Medikai rendszerek

3.1.4.2.1.11. Helyreállítás

Az alternatív rendszer indításához a DRP-ben található, rendszerenként eltérő adatbázisokra van szükség.
Ezen adatbázisok kinyerhetőek az éles rendszer mentéseiből.

3.1.4.3. A folyamatos működésre felkészítő képzés

3.1.4.3.1. Az érintettek meghatározása

Az Intézmény az elektronikus információs rendszer folyamatos működésére felkészítő képzést tart a felhasználóknak; szerepkörüknek és felelősségüknek megfelelően.

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 Az Intézmény 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

Az Intézmény 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 a Igazgató egyedi döntése alapján optikai adathordozóra is menthetők, de ebben az esetben legalább 2 másolatot kell készíteni.

3.1.4.8.1.2. A mentések gyakorisága

Az Intézmény 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.

3.1.4.8.1.3. Dokumentációk mentése

Az Intézmény 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, verziószám megjelöléssel tarolandók.

3.1.4.8.1.4. A mentések tárolásának alapelvei

Az Intézmény 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.

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

3.1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása

3.1.4.9.1. A helyreállítás

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

3.1.5 A Biztonsági események kezelése

3.1.5.1.1. Eseménykezelési eljárás

A felhasználó kötelcs az általa tapasztalt rendellenes eseményeket az üzemeltetővel azonnal közölni, szóbeli közlés esetén legkésőbb a következő munkanapon írásban is megerősíteni. Kötelcs 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 kötelcs azonnal jelezni ezt az üzemeltető felé, továbbá amennyiben a lehetőségei adottak, köteles a jelszavát azonnal megváltoztatni, személyazonosító eszközét letiltatni a megfelelő szolgáltatónál.

3.1.5.1.2. Egyeztetés

Az Intézmény egyezteti az eseménykezelési eljárásokat az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel.

3.1.5.1.3. Következtetések

Az Intézmény 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.

3.1.5.6.1.2. Hatósági bejelentés

Az Intézmény 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

3.1.5.7.1. Support

Az Intézmény 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

3.1.5.8.1.1.1. Kezelési módok

Az Intézmény a biztonsági eseményeit súlyosságuk szerint priorizálja, és ennek megfelelően kezeli.

3.1.5.8.1.1.2. Lehetőségek

Az Intézmény 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 igénybe vételére 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

Az Intézmény 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

Az Intézmény lehetőségeihez mérten kielégíti, a biztonsági események kapcsán az informatika szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit.

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 e-mailen 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 értékek 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

Az Intézmény 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 Az Intézmény 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

Az Intézmény a biztonsági eseménykezelési terv változásait a 3.1.5.8.1.2. pont szerint ismerteti.

3.1.5.8.1.6. Bizalmasság

Az Intézménynek 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

Az Intézmény 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 az Intézmény teljes személyi állományára, valamint minden olyan természetes személyre, aki Az Intézmény elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges vagy feltételezhető kapcsolatba kerülő személy nem Az Intézmény 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).

3.1.6.2. Munkakörök, feladatok biztonsági szempontú besorolása

3.1.6.2.1.1. Besorolások (worktable)

Az Intézmény 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

Az Intézmény 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

Az Intézmény 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

Az Intézmény 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 Az Intézmény 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

Az Intézmény folyamatosan ellenőrzi a 3.1.6.3.1. pont szerinti feltételek fennállását.

3.1.6.4 Eljárás a jogviszony megszűnésekor

3.1.6.4.1.1. Hozzáférések megszüntetése

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 Az Intézmény alkalmazottjának munkaviszonya, „rendes" felmondás keretein belül megszűnik, erről a tényről a közvetlen felettesének, illetve a felmondást aláíró vezetőnek haladéktalanul tájékoztatást kell nyújtania az informatikai osztálynak. Az informatikai osztály a jelzett időponttal gondoskodik a felhasználó összes rendszerhozzáférésének adott időpontban történő megszüntetéséről vagy letiltásáról, illetve ezek kezdeményezéséről. Az eljárás megtörténtéről az informatikai osztály 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 informatikai osztályt. Az informatikai osztály tájékoztatásáért egyetemlegesen felel a felmondást szignáló személy és a munkaügyi ügyintéző. Az informatikai osztálynak 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

Az Intézmény 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

Az Intézmény 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

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

3.1.6.4.1.5. Folytonosság

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

3.1.6.4.1.6. Értesítés

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

3.1.6.4.1.7. Titoktartás

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

3.1.6.4.1.8. Jogsértések megelőzése

Az Intézmény 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

Az Intézmény szükség esetén elvégzi a 3.1.6.3. pontban foglalt, a személyek ellenőrzésére vonatkozó eljárást.

3.1.6.5.1.2. Engedélyezési eljárás

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

3.1.6.5.1.3. Felülvizsgálat

Az Intézmény szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését.

3.1.6.5.1.4. Tájékoztatás

Az Intézmény az általa meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

3.1.6.6. Az Intézménnyel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

3.1.6.6.1.1. Felelősségek, Feladatok meghatározása

Az Intézmény 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 vállalat rendszereinek informatikai vagyonát leltárlisták tartalmazzák. Ezek alapként szolgálnak a kockázatelemzéshez és a védelmi intézkedések meghatározásához.
Az Intézmény 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

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

3.1.6.6.1.3. Dokumentációs követelmények

Az Intézmény a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket.

3.1.6.6.1.4. Tájékoztatási kötelezettség

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

3.1.6.6.1.5. Ellenőrzés

Az Intézmény folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.