Ikt.: 91511-A/2182/2020

Szabolcs-Szatmár-Bereg

Megyei Gyermekvédelmi Központ

Informatikai Biztonsági Szabályzata

2020.év

Készítette: Prekub Zsolt
adatvédelmi tisztviselő

Jóváhagyta: Repelik Anikó
intézményvezető

1. Cél

Az Informatikai Biztonsági Szabályzatának (IBSZ) célja, hogy a vonatkozó jogszabályokkal, a **Szabolcs-Szatmár-Bereg Megyei Gyermekvédelmi Központ (továbbiakban Intézmény)** belső szabályzataival, minőségirányítási rendszerével összhangban meghatározza azIntézmény informatikai rendszerei által kezelt információvagyon bizalmassága, sértetlensége, valamint rendelkezésre állásának biztosítása és üzemeltetési és információbiztonsági folytonosságának megőrzése érdekében betartandó elveket. Az IBSZ meghatározza az Intézmény informatikai rendszerének üzemeltetőinek, az Intézmény állományába tartozó munkatársainak, beszállítóinak, szerződött munkatársainak feladatait, a számukra meghatározott szabályokat.

A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét, információvédelmi szabályokat határoz meg, valamint ellenőrzési mechanizmusokat állít fel a nem megfelelőségek észlelésére és a felelősség megállapítására.

Az IBSZ továbbá:

- azIntézmény által kezel munkavállalói, partneri, vevői személyes adatok védelmének megteremtésére, fenntartására.
- a vagyonvédelemre (ide tartoznak azIntézmény adatvagyonának, információs vagyonának elemei is) és tűzvédelemre vonatkozó védelmi intézkedése betartása.
- az üzemeltetett informatikai rendszerek rendeltetésszerű üzemeltetése és használata.
- folyamatos karbantartás,
- az adatok feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszűntetése, minimalizálása.
- az adatok tartalmi és formai épségének megőrzése, biztonságos mentése.
- a lekérdezhető adatok körének meghatározása.
- az adatfeldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása.
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

2. Alkalmazási terület

2.1. Személyi hatály

A szabályozás személyi hatálya kiterjed azIntézmény minden alkalmazottjára, alvállalkozóinak munkatársaira, és mindazon felhasználóira, akik hozzáférési jogosultsággal rendelkeznek az informatikai rendszerekhez és információ tároló, feldolgozó helységekhez (pl: irattár, tervtár).

2.2. Területi hatály

Az IBSZ a tárgyi hatálya alá tartozó elemek tejes életciklusára kiterjed, amely az alábbi szakaszokból áll:

- tervezési szakasz
- fejlesztési szakasz
- megvalósítási szakasz
- üzemeltetési szakasz
- visszavonási, selejtezési és megsemmisítési szakasz

A szabályozás területi hatálya az alábbi területekre terjed ki:

- azIntézményszakmai egységei és vagy különleges munkarend esetében munkavégzési külső helyszínei
- a védelmez élvező elektronikus és papír alapú adatok teljes körére, létrehozási helyétől, feldolgozási helyétől (pl: külső bérszámfejtő partner), idejétől és az adatok fizikai formájától függetlenül.
- azIntézmény tulajdonában lévő, illetve az általa bérelt, lízingelt valamennyi informatikai berendezésre.
- azIntézmény által használt szoftverek, hardverek műszaki dokumentációira
- az összes dokumentációira (fejlesztési, üzemeltetési, felhasználói dokumentumok.
- az operációs rendszerekre, azok környezetére.
- az adatok - különös tekintettel a személyes adatok - felhasználására vonatkozó eljárásokra.
- az elektronikus és papír alapú adathordozók tárolására, felhasználására.

3. Fogalmak

A fogalmak az ISO/IEC 27000 szabvány hatályos fogalomtárára épül.

A személyes adatok kezelésével kapcsolatos fogalmakat az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a " természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) " 4. cikk " Fogalommeghatározások " cikk tartalmazza.

4. Kapcsolódó szabályozások, jogszabályok

Jelen IBSZ- hez kapcsolódó jogszabályok, belső előírások:

- MSZ ISO/IEC 27001:2013 szabvány
- az Európai Parlament és a Tanács (EU) 2019/679 rendelete
- 2013. évi L. törvény
- 41/2015 (VII.15.) BM rendelet
- azIntézmény mindenkor érvényes SZMSZ-e

5. Információbiztonsági szabályok

5.1. Az információbiztonság vezetői irányítása

5.1.1. Információbiztonsági szabályok

AzIntézmény megfogalmazza és kihirdeti az informatikai biztonságpolitikát, melyben meghatározza az információvédelmi célokat, kifejti az alkalmazott informatikai biztonsági alapelveket és megfelelőségi követelményeket, valamint bemutatja a vezető beosztású tagjainak elkötelezettségét a biztonsági feladatok irányítása és támogatása iránt.

5.1.2 Az információbiztonsági szabályok átvizsgálása

Az információvédelmi politika felülvizsgálata és esetleges frissítése évente legalább egyszer, vagy az IT rendszert értintő változások esetén esedékes.

6. Az információbiztonság szervezete

6.1 Belső szervezet

Az informatikai biztonsággal kapcsolatos feladatok szerepkörökhöz rendeltek. A szerepkörök szerinti felelősök kijelölése a munkaköri leírásokban történik.

6.1.1. Információbiztonsági szerepek és felelősségek

Az információvédelemi vezető (CISO) feladatai:

- A CISO szervezeti vezetői támogatással biztosítja az e szabályzatban meghatározott követelmények teljesülését
- közreműködik azIntézmény információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázat elemzésében és kockázatkezelésében, karbantartásában, hibaelhárításában és fejlesztésében
- az IBSZ kezelése, naprakészen tartása, módosítása
- javaslatot tesz a rendszer kockázatainak felszámolására
- javaslatot tesz a védett adatok körének meghatározására
- ellenőrzi az információvédelmi előírások betartását
- meghatározza a rendszerek biztonsági beállításával kapcsolatos elvárásokat, jogokat, feladatokat
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából azIntézménye tárgykört érintő szabályzatait és szerződéseit
- feladata az információvédelmet támogató nyilvántartási rendszer kialakítása és működtetése
- részt vesz a belső auditokon
- ellenőrzi a szoftverek használatának jogszerűségét

Az informatikai üzemeltetési vezető (CIO) feladatai az információvédelemhez kapcsolódóan:

- a saját feladat körébe tartozó rendszerek felügyelete
- felelős az informatikai rendszerek üzembiztonságáért
- felelős a szerverek adatairól biztonsági másolatok készítéséért, teszteléséért, és karbantartásáért
- feladata a védelmi eszközök, felügyeleti rendszerek működésének folyamatos ellenőrzése
- felelős azIntézményi informatikai rendszerének hardver és szoftver eszközeinek karbantartásáért
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver elemeket

- gondoskodik a folyamatos vírusvédelemről szerver, munkaállomás és mobiltelefon szinten
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges jellemzők alakulását
- ellenőrzi a rendszer adminisztrációját

A felhasználók feladatai:

- ismerniük kell az Informatikai Biztonsági Szabályzatban szereplő előírásokat és azokat be kell tartaniuk
- rendelkezniük kell az általuk üzemeltetett berendezésekre és szoftverekre vonatkozó előírásokkal, illetve ismerniük kell azok tartalmát
- tevékenységük megkezdésekor ellenőrizni kell, hogy az általuk használt eszközök üzemképesek- e és azok beállítása az előírásoknak megfelelő-e, nem észlelnek-e furcsa tevékenységet, riasztást
- kötelesek figyelemmel kísérni az általuk használt informatikai eszközök és szoftverek állapotát és az esetleges meghibásodást vagy helytelen működést azonnal jelezni kell
- munkájuk során figyelni kell arra, hogy illetéktelen személyek lehetőleg ne tartózkodjanak a helyiségben.
- tevékenységük befejezésekor a használt szoftverekből szabályszerűen ki kell lépni, a számítógépieket lockolniuk kell
- az eszközöket szükség esetén az előírásoknak megfelelően le kell állítani, illetve áramellátását meg kell szűntetni
- a helyiségből utolsóként való távozáskor meg kell győződni a helyiség biztonságos lezárásáról

6.1.2. Feladatkörök szétválasztása

6.1.3. Kapcsolat a hatóságokkal

6.1.4. Kapcsolat szakmai csoportokkal

6.1.5. Információbiztonság a projektvezetésben

6.2. Mobil eszközök és távmunka

6.2.1. Szabály mobil eszközökre

6.2.2. Távmunka

7 Az emberi erőforrások biztonsága

7.1. A munkaviszony kezdete előtt

7.1.1. Átvilágítás

7.1.2 A munkaviszonnyal kapcsolatos feltételek és kikötések

AzIntézmény meghatározza a felvételi eljárás során követendő szabályokat, személyes követelményeket. A követelményeket a Munkaköri leírásokban rögzíti.

7.2. A munkaviszony fennállása során

7.2.1. Vezetői felelősségek

7.2.2. Az információbiztonság tudatosítása, oktatása és képzése

Az új belépő munkatársa belépéskori oktatás és a titoktartási nyilatkozat aláírása után kaphat hozzáférést a rendszerekhez. A belépő munkatárs új hozzáférési jogkörét, illetve átszervezésben érintett saját munkatárs hozzáférési jogkör változtatását a felettes vezetője határozza meg.

A meghatározás során az érintett vezető a hozzáférések igénylése és letiltása formanyomtatványon összegzi az általa szükségesnek tartott hozzáféréseket és azokat jóváhagytatja az illetékes Intézményvezető helyettessel. Amennyiben az illetékes Intézményvezető helyettes nem járul hozzá a kért jogosultságok kiadásához, úgy az ahhoz való hozzáférést megtilthatja, de ezen döntését indokolnia kell az igénylő felé.

A jóváhagyott formanyomtatványt az igénylő vezető továbbítja az értintett rendszer adminisztrátora felé, akinek felelőssége, hogy csak a jóváhagyott jogosultságot állítsa be. A rendszergazdának tilos az engedélyben nem szereplő jogosultságokat beállítania. A beállítások megfelelőségét alkalmanként a CISO ellenőrizheti.

Amennyiben az információ biztonsági szabályozásban feladat és felelősségi köröket érintő változások következnek be, úgy a változtatásokat vezetői jóváhagyás után át kell vezetni a munkaköri leírásokba és azokat aláírással érvényesíttetni az érintettel. Amennyiben a módosított munkaköri leírásokkal kapcsolatban az érintett munkavállalónak észrevétele van, azt a CISO felé teheti meg.

Amennyiben a változások vállalkozói szerződéseket érintenek, úgy azIntézmény beszerzési vezetője kezdeményezi az érintett vállalkozói szerződések módosítását, illetve kiegészítését a biztonsági követelményeknek megfelelően és menedzseli a szerződések módosítását és azokat aláírással történő érvényesítését, mely munkában közreműködik a CISO.

Új munkakörök kialakítása során az illetékes Intézményvezető helyettes tájékoztatja a CISO-t az új munkakör feladatairól és tervezett jogosultságairól. A CISO javaslattal élhet a munkakör feladatainak biztonsági vonatkozásait illetően.

A felhasználókat az információvédelem megvalósítása érdekében munkakörüknek megfelelően képezni kell, a fejlesztői, üzemeltetői munkatársaknak pedig folyamatosan szinten kell tartania, és fejleszteni kell az informatikával és információvédelemmel kapcsolatos ismereteit. A felhasználókat naprakészen képezni kell az új IT eszközök, alkalmazások bevezetésekor. AzIntézményben alkalmazott új dolgozót soron kívül ki kell oktatni az informatikai rendszerek használatáról.

A követelmények, és a ténylegesen rendelkezésre álló erőforrások összevetése alapján évente

oktatási tervet készít a HR vezető. Ez tartalmazza a szükséges oktatásban résztvevők körét, az oktatás téma körét és követelményeit. A tervezett képzéseknél figyelembe kell venni a minőségi, környezeti, a munkahelyi egészségvédelmi és biztonsági, illetve információvédelmi célok kapcsán megfogalmazott, a jövőben elvárt kompetenciákat is.

7.2.3. Fegyelmi eljárás

A biztonsági előírásokat megsértőkkel szemben fegyelmi eljárás indul. Fegyelmi eljárást az érintett munkavállaló közvetlen vezetője, a CISO, és az Intézményvezető kezdeményezhet. A kezdeményezésnek tartalmaznia kell:

- a fegyelmi eljárást kezdeményező nevét, beosztását
- a valószínűsíthető vétséget elkövető nevét, beosztását
- az észlelés idejét
- a fegyelmi vétség elkövetésének feltételezett idejét, módját, körülményeit
- a keletkező károk, és egyéb következmények leírását

Az Intézményvezető a kezdeményezést elbírálja, melyről értesítést küld a kezdeményezőnek, és a CISO-nak. Kitűzi továbbá a fegyelmi eljárás megbeszélésének időpontját, és meghatározza azon részt vevő személyek körét.

Az érvényesítés során azIntézmény vezetőjének állásfoglalására alapozva a szükséges teendők meghatározásra kerülnek. Ezen feladatokat a fegyelmi eljárás jegyzőkönyvére kell felvezetni.

Amennyiben az elektronikus információbiztonsági szabályokat nem azIntézmény személyi állományába tartozó személy sérti meg, úgy azIntézmény érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépéseket, szükség szerint bevezeti ezeket az eljárásokat.

7.3. Munkaviszony megszűntetés és megváltoztatása

7.3.1. A munkaviszony megszüntetéséhez és megváltoztatásához kapcsolódó felelősségek

A munkavállaló vagy szerződéses partner jogviszonyának megszűnése esetén a munkavállaló felettes vezetője gondoskodik a kilépő munkavállaló vagy szerződéses partner IT rendszerrel vagy annak biztonságával kapcsolatos feladatainak ellátásáról a jogviszony megszűnését megelőzően. A jogviszony megszűnések a CISO gondoskodik arról, hogy a kilépő esetleges IT rendszert, illetve az abban tárolt adatokat értintő információvédelmi szabályokat sértő magatartást megelőzze. (hozzáférések megszűntetése, jogosultságok visszavonása)

A CISO a kilépő számára igazolja, hogy a hozzáférési jogokat törölte, illetve az illetékes szervezeti vezetők aláírásukkal igazolják a kilépő lapon, hogy a kilépett felhasználó azIntézmény felé elszámolt. A kilépőt továbbá tájékoztatni kell az esetleg rá vonatkozó, jogi úton is kikényszeríthető a jogviszony megszűnése után is fennálló kötelezettségekről. AzIntézmény meghatározott ideig megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz a személyes adatok védelmével összhangban.

8. Vagyonelemek kezelése

8.1 A vagyonelemekért vállalt felelősségek

8.1.1 Vagyonleltár

Az adatbiztonság szempontjából azIntézmény kezelésében lévő elektronikus formában tárolt információkat, eszközöket, erőforrásokat és szolgáltatásokat a kezelt adatok bizalmassága, sértetlensége, és rendelkezésre állása szempontjából 1-től 5-ig terjedő skálán - a kockázat növekedésével arányosan növekvő - biztonsági osztályba kell sorolni. A besorolás eredményét melléklet formában rögzíteni kell az IT leltárban is.

Ezt a besorolást minimum két évente, vagy az IT rendszereket érintő változások után, illetve jogszabály, vevői igény változás esetén felül kell vizsgálni és szükség esetén ismételten el kell végezni.

8.1.2 A vagyonelemek felelősei

8.1.3. A vagyonelemek elfogadható használata

8.1.4 A vagyonelemek visszaszolgáltatása

8.2. Információosztályozás

8.2.1. Az információk osztályozása

Az adatokat és az információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- nyílt, bárki által megismerhető adatok
- bizalmas adatok

8.2.2 Az információk megjelölése

A keletkező adatok minősítője annak létrehozója vagy a CISO. Az adatok létrehozásakor meg kell határozni a hozzáférési jogosultságot. A kijelölt munkatársak, alvállalkozói partnerek, tanácsadók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját, és időtartamát ismertetni kell.

8.2.3 A vagyonelemek kezelése

AzIntézmény célja, hogy mindenki csak ahhoz az adathoz férhessen hozzá, melyekre a munkájához feltétlenül szükség van. Az információhoz való hozzáférést a tevékenység naplózásával dokumentálja az IT üzemeltetés, ezáltal bármely számítógépen végzett tevékenység - adatbázisokhoz való hozzáférés, a fájlba, vagy mágneslemezre illetve külső egységre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet - utólag visszakereshető.

8.3 Adathordozók kezelése

AzIntézménynél az adathordozók kezelésére az alábbi szabályok vonatkoznak:

- jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak

- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni, melynek felelőse a CISO
- a használni kívánt adathordozót (papír, USB, CD, DVD, egyéb adathordozó, merevlemez, stb.) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni
- az asztalon csak azok a papír és elektronikus adathordozók legyenek, amelyek az aktuális munka elvégzéséhez szükségesek
- adathordozót másnak átadni csak engedéllyel szabad
- a munkák befejezésekor a használt informatikai eszközt és annak közvetlen környezetét rendbe kell tenni, figyelve a tiszta asztal, tiszta képernyő politikára.

8.3.1. A cserélhető adathordozók kezelése

AzIntézmény által használt hordozható külső adattárolókat (USB, pendrive-ok, memóriakártyák, CD/DVD-k, hordozható hdd-k és ssd-k) egyedi azonosítóval kell ellátni. Az egyedi azonosítóval ellátott hordozható adathordozók pontos helyéről naprakész adatbázist kell vezetni.

A használni kívánt adattárolót a tárolásra kijelölt helyről kell kivenni és használatot követően oda kell visszahelyezni. A munkaasztalokon csak azok az adathordozók lehetnek, amelyek a munkavégzéshez szükségesek.

Fontos adatokat tartalmazó adathordozókról másolatot kell készíteni, melyet egymástól elkülönítetten, lehetőleg külön szobában jól zárható lemezszekrényben kell elhelyezni.

Az adathordozókról az illetékes osztályvezetőnek nyilvántartást kell vezetni. Az adathordozókat a biztonság érdekében azonosítóval kell ellátni. Az adathordozók tárolására műszaki-, tűz-, és vagyonvédelmi előírásoknak megfelelő eszközt (pénzkazettát, papírdokumentumok bizalmas tárolására alkalmas eszközt) kell kialakítani. Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségének megfelelően kell megvalósítani. Ezekről a szabályokról azIntézményi jogász ad információt.

8.3.2. Adathordozók eltávolítása

A selejtezést a vállalkozás selejtezésének szabályzata alapján kell lefolytatni. Sokszorosítást, másolást, csak az érvényben lévő belső utasítások szerint szabad végezni.

8.3.3. Fizikai adathordozók szállítása

9. Hozzáférés felügyelet

9.1. A hozzáférés felügyelettel kapcsolatos üzleti követelmények

A hozzáférési jogosultságok igénylő felhasználóval szembeni elvárásokat, a rá vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységeket jelen dokumentum, valamint az adott rendszerdokumentáció tartalmazza. A hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő személynek írásbeli nyilatkozatot kell tennie arról, hogy az érintett rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

9.1.1 Szabály a hozzáférés- felügyeletre.

9.1.2 Hozzáférés hálózatokhoz és hálózati szolgáltatásokhoz

9.2. Felhasználói hozzáférések kezelése

AzIntézményi hozzáférések kezelését azIntézményi hozzáférések kezelése szabályzat szabályozza részletesen.

9.2.1. Felhasználók regisztrálása és törlése

A szolgáltatás tulajdonos által definiált hozzáférés-védelem elve szerint a szolgáltatás tulajdonosa által meghatározott szabályok (engedélyezés) alapján kell az adott szolgáltatáshoz történő hozzáférési jogosultsági kört kialakítani. A szolgáltatás tulajdonosa által megfogalmazott szabályok alapján kell beállítani a megfelelő hozzáférési módot. A jogosultságok beállítását az informatikai rendszerbet az IT végzi el.

9.2.2. Felhasználói hozzáférés biztosítása

9.2.3 Kiemelt hozzáférési jogok kezelése

A munkaállomásokon és szervereken telepített szoftverek / alkalmazások és szakalkalmazások esetében kiemelt figyelmet kell fordítani az automatikusan létrejövő felhasználókra, hozzáférésekre, jogosultságokra, ezek kezdeti jelszavát meg kell változtatni. Figyelmet kell fordítani a „ teszt jelleggel „ létrehozott felhasználókra, hozzáférésekre. Ezeket a felhasználókat, hozzáféréseket, amikor használatuk már nem szükséges, és indokolt meg kell szűntetni. Amennyiben a hozzáférések szükségesek, úgy legalább a magasabb szintű biztonságukról gondoskodni kell, így vagy át kell őket nevezni, vagy a nem szükséges jogosultságokat el kell venni ezektől a felhasználóktól. Az ilyen felhasználók alapértelmezett jelszavait meg kell változtatni megfelelő erősségű jelszavakra.

9.2.4. A felhasználók titkos hitelesítési információinak kezelése

9.2.5. A felhasználói hozzáférési jogok átvizsgálása

Az IT rendszerhez történő hozzáférési engedélyeket évenként felül kell vizsgálni. Az esetlegesen már nem indokolt jogosultságokat, hozzáféréseket meg kell szűntetni.

9.2.6. A hozzáférési jogok visszavonása vagy módosítása

A felhasználó szerepkörének megváltozása esetén az IT a kapott információk alapján a régi szerepkörökhöz tartozó jogosultságot a felhasználótól elveszi, majd a szükséges új szerepkörnek megfelelő jogosultságokat megadja neki.

A felhasználó jogviszonyának megszűnése esetén a CISO igazolja a HR munkatárstól kapott

nyomtatványon, hogy a hozzáférési jogokat törölte, illetve a felhasználó az informatikai vezető felé elszámolt.

9.3 Felhasználói felelősségek

9.3.1 Titkos hitelesítési információk használata

A felhasználók kizárólag felhasználói jogosultsággal dolgozhatnak a munkaállomásokon, rendszergazdai jogosultságokat nem kaphatnak. Az így rendelkezésre álló jogokat a felhasználó nem használhatja semmilyen üzemeltetői feladatra, csak és kizárólag az IT rendszer használata miatt birtokolhatja ezeket! A felhasználók kötelesek felhasználói azonosítójukat bizalmasan kezelni, azt más személynek nem adhatják át.

9.4. Rendszer- és alkalmazás – hozzáférés felügyelete

9.4.1 Információhoz való hozzáférés korlátozása

9.4.2 Biztonságos bejelentkezési eljárások

9.4.3 Jelszókezelő rendszer

9.4.4 Kiemelt jogokkal bíró segédprogramok használata

Azon munkatársak munkaállomásai, ahol valamely célszoftver, laboratóriumi eszköz működéséhez szükségesek az emelt szintű jogok, itt a zavartalan munkavégzés miatt ez engedélyezett. Az igy rendelkezésre álló jogokat a felhasználó nem használhatja semmilyen üzemeltetői feladatra, nem élhet vissza vele, nem telepíthet programokat!

9.4.5 A programok forráskódjához való hozzáférés felügyelete

10. Titkosítás

10.1 Titkosítási intézkedések

10.1.1 Szabály a titkosítási intézkedések tételére

Az IT rendszer szabványos és biztonságosnak minősített kriptográfiai műveleteket valósít meg. Az IT rendszer meggátolja az együttműködésen alapuló informatikai eszközök (kamerák, mikrofonok) távoli aktiválását, kivéve ha a szervezet engedélyezte azt, közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

10.1.2 Kulcskezelés

11. Fizikai és környezeti biztonság

A fizikai és környezeti biztonsági vonatkozó óvintézkedések azIntézményi rendszereknek helyet adó épületekkel, a rendszer erőforrásokkal és a működést biztosító alapszolgáltatásokkal kapcsolatban fogalmaznak meg szabályokat annak érdekében, hogy az IT szolgáltatások megszakadását, eszközök illetéktelen kivitelét azIntézménytől, a fizikai károkozást, az információk jogosulatlan felfedését, a rendszer sértetlenségének elvesztését megakadályozzák.

11.1 Biztonsági területek

11.1.1 Fizikai biztonsági határ

AzIntézmény székhelyénés szakmai egységeiterületén biztonsági zóna nincs kijelölve

11.1.2 Fizikai beléptetési intézkedések

Az IT rendszereknek helyt adó területekre való belépésre jogosultakról a CISO nyilvántartást vezet és belépési jogosultságot igazoló eszközöket oszt ki számukra.

11.1.3 Irodák, helyiségek és létesítmények védelme

Azon helyiségek kijelölése, illetve kialakítása során, amelyekben azIntézmény kiemelt fontosságú IT eszközei (szerverei) és papír alapú adathordozói, mentései kerülnek elhelyezésre, különös figyelmet kell fordítani a fokozott biztonságra.

11.1.4.Külső és környezeti fenyegetésekkel szembeni védelem

11.1.5.Munkavégzés biztonsági területeken

A kiemelt biztonságú helyiségek (irattár, tervtár, szerverszoba) közelében nem üzemelhet tűz- és robbanásveszélyes raktár, A helyiségben tűzjelző rendszert kell kiépíteni, amelynek üzembiztonságát az előírásoknak megfelelően időszakosan ellenőrizni kell.

A helyiséget mindig zárva kell tartani. A helyiség kulcsait munkaidőben csak CISO vagy a CIO, illetve a CIO által felhatalmazott személy veheti fel, mivel a szerver sértetlensége, rendelkezésre állása az ő felelősségük. A felvétel tényét minden esetben nyilván kell tartani. Munkaidőn kívül a kulcsokat elzártan kell tartani. A helyiségben idegen személy felügyelet nélkül nem tartózkodhat. A belépésre jogosultak listáját mindig naprakészen kell tartani, akinek a belépése már nem indokolt el kell távolitani a listáról, a belépési jogosultságot igazoló dokumentumait és eszközeit vissza kell vonni.

11.1.6 Szállítási és rakodási területek

11.2 Berendezés

11.2.1 Berendezések elhelyezése és védelme

AzIntézményi informatikai eszközöket és adathordozókat lopás, rongálás, megsemmisülés ellen kockázatokkal arányosan védeni kell (élőerős védelem az irodaházi biztonsági szolgálat részéről és fizikai védelmi intézkedésekkel a rácsok, ajtók a biztonsági szolgálathoz bekötött riasztóberendezés segítségével) A hardverek és adatok részleges vagy teljes megsemmisülésével fenyegető tűzek megelőzése és elhárítása az irodaház tűzvédelmi szabályzatainak rendelkezései szerint történik.

Az infrastrukturális gyengeségek és hiányosságok kivédése érdekében az egyes rendszerek rendelkezésre állási biztonsági osztályba sorolása után gondoskodni kell a megfelelő infrastruktúra biztosításáról. Ilyenek lehetnek a következők: szünetmentes áramellátás, hőmérséklet és páratartalom szabályozó rendszer, biometrikus beléptető rendszer a kritikus helységekre.

11.2.2 Közműszolgáltatások

11.2.3 Kábelbiztonság

11.2.4 Berendezések karbantartása

AzIntézmény megfogalmazza, és azIntézményre érvényes követelmények szerint dokumentálja, valamint a szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A fizikai védelmi szabályozásban, vagy más belső szabályozásban meghatározott gyakorisággal felülvizsgálja és frissíti a karbantartási eljárásrendet. A CIO feladatai az alábbiak:

- jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen vagy másutt tartják karban.
- felelős személyek jóváhagyásához köti az IT rendszer vagy rendszerelemek kiszállítását a szervezeti épületekből.
- az elszállítás előtt minden adatot és információt - mentést követően – töröl a berendezésről amennyiben az technikailag lehetséges.
- ellenőrzi hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e
- biztonsági ellenőrzésnek veti alá a visszaérkezett IT eszközöket
- csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz

11.2.5 Vagyonelemek eltávolítása

11.2.6 Berendezések és vagyonelemek biztonsága a szakmai egységein kívül

AzIntézményi tulajdonban lévő (vagy azIntézmény által bérelt, lízingelt) behozni vagy kivinni szándékozott IT berendezések mozgatása (pl: javítás céljából, mobil egységek, laptop) csak Intézményi érdekből lehetséges, amelyet a CISO vagy az illetékes Intézményvezető helyettes engedélyezhet. Ezeket az eseményeket dokumentálni kell. Nem kell alkalmanként dokumentálni a személyes használatra, név szerint, tartósan átadott eszközök mozgatását.(pl: céges laptopok, telefonok)

A javítás céljából azIntézménytől kikerülő eszközök esetében biztosítani kell, hogy azIntézmény által kezelt adatok ne kerüljenek ki. Olyan meghibásodott eszközök (fényképezőgépek a MEO-tól, pc, mobil eszközök, szerverek) amelyekben az adathordozók védendő adatokat tartalmazhatnak nem kivihetőek együtt az adathordozó alkatrésszel. Ebben az esetben az adathordozót (merevlemez, statikus memória egység, stb.) a javítás idejére csereeszközzel kell a gépen helyettesíteni vagy ha nem szükséges ez az alkatrész a működéshez, akkor az eredeti adathordozó és cserealkatrész nélkül kell javítási célból kivinni. Az eredetileg használt adathordozót a javítás után vissza kell helyezni az eszközbe, vagy arról az adatokat az új eszközre át kell tenni amennyiben az lehetséges.

11.2.7 Berendezések biztonságos eltávolítása vagy újra felhasználása

Az adathordozók biztonságához szorosan kapcsolódik az, hogy az adathordozók újra használása, illetve selejtezése után is biztosítani kell a védendő adatok bizalmasságát.

Amennyiben adathordozó eszközök (USB, pendrive-ok, memóriakártyák, hordozhatók hdd-k és ssd-k) újra felhasználásra kerülnek úgy biztosítani kell hogy az új felhasználó jogosulatlanul ne férjenek hozzá a korábban az eszközön tárolt adatokhoz. Ebben az esetben az eszközökön biztonságos törlést kell végrehajtani, úgy hogy a teljes adathordozón található valamennyi adat legalább háromszor kerüljön felülírásra véletlen adatfolyammal. A tárolók tartalmát, hogy az adathordozó törlése sikeres volt-e, a CISO minden esetben ellenőrzi. Azokat az adathordozókat melyeket nem lehet engedélyezett módon törölni, újra felhasználni tilos, az ilyen eszközöket meg kell semmisíteni.

Amennyiben az adathordozó oly mértékben sérült vagy elhasználódott, hogy a további használata lehetetlen vagy célszerűtlen, úgy azt selejtezni majd megsemmisíteni kell.

A selejtezési eljárás folyamán az adathordozókon olyan eljárást kell végrehajtani, amelyek megakadályozzák azt, hogy a későbbiekben ezekről az eszközökről adatokat lehessen visszanyerni. Ennek megfelelően a következő adat megsemmisítési módszerek kerülnek meghatározásra: floppy, CD, DVD, pendrive-ok, statikus memóriák esetén az erre alkalmas adatmegsemmisítő eszközzel be kell zúzni azokat. Merevlemezek esetén pedig a mágneslemezt el kell távolítani az eszközből, majd a CD, DVD lemezek esetén is használatos adatmegsemmisítő eszközzel be kell zúzni azt.

11.2.8 Őrizetlenül hagyott felhasználói berendezések

11.2.9 Tiszta asztal és tiszta képernyő szabálya

12. Az üzemelés biztonsága

12.1 Üzemeltetési eljárások és felelősségek

12.1.1 Dokumentált üzemeltetési eljárások

12.1.2 Változásfelügyelet

A változáskezelés célja, hogy azIntézményi informatikai rendszerének (hardver, szoftver, folyamatok, szabályzatokstb.) bármilyen fejlesztése, átalakítása:

- tervezetten
- azIntézményi informatikai stratégiához és informatikai ajánlásokhoz illeszkedően, tervezhető költségekkel
- szervezett keretek között történjen

A változáskezelés gazdái a CISO és CIO a saját területük vonatkozásában

12.1.3 Kapacitáskezelés

12.1.4 A fejlesztési, tesztelési és az üzemi környezetek elkülönítése

12.2 Védelem a rosszindulatú szoftverek ellen

12.2.1 Intézkedések a rosszindulatú szoftverek ellen

12.3 Mentés

12.3.1 Információk mentése

A munkavégzés során folyamatosan biztosítani kell az adatok mentését. A munka során létrehozott általános Word, Excel és PowerPoint dokumentumok mentése az azt létre hozó munkatársak (felhasználók) feladata. A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak. A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért a CIO felelős.

AzIntézményi mentési szabályzat bővebb információkat tartalmaz.

12.4 Naplózás és megfigyelés

12.4.1 Eseménynaplózás

AzIntézmény az IT rendszereinek tervezésekor is már rögzített naplózási szabályokat kell alkalmazni.

Ennek során az alábbi alapelveknek kell megfelelni:

- az IT rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg
- az elszámoltathatóság érdekében a naplózási funkciókat úgy kell beállítani, hogy a felhasználói tevékenységek személyre szólóan nyomon követhetőek legyenek a GDPR szabályainak megfelelően
- az események és problémák azonosítása érdekében a napló tartalmazza a problémák megoldásához szükséges adatokat
- a visszaélések felderítése érdekében a jogosult felhasználói tevékenységek és jogosulatlan tevékenységekre irányuló kísérletek naplózásra kerülnek
- az IT rendszerekben megbízható módon védeni kell az ott keletkezett naplóállományokat, a jogosulatlan felfedés, módosítás és törlés ellen
- a naplóállományok ellenőrzését a CIO végzi. Az ellenőrzések rendszeresen, legalább kéthetente kell megtörténnie. Az ellenőrzések hatékonyságának növelésére automata ellenőrző szoftvert is lehet alkalmazni, amennyiben ez az adott rendszeren technikailag lehetséges.

12.4.2 Naplóinformációk védelme

Informatikuson túl a naplóállományok adattartalmába betekinthetnek:

- CIO
- CIO vagy CISO valamelyike által írásban felhatalmazott szakember

Az IT rendszert úgy kell felépíteni, hogy az megvédi a naplóinformációt és a napló-kezelő eszközöket a jogosulatlan hozzáféréssel , módosítással és törléssel szemben.

12.4.3 Adminisztrátori és operátori naplók

12.4.4 Óraszinkronizálás

12.5 Az üzemelő szoftverek felügyelete (Control of operational software)

12.5.1 Szoftverek telepítése az üzemelő rendszerekre (Installation of software on operational systems)

12.6 A műszaki sebezhetőségek felügyelete

12.6.1 Műszaki sebezhetőségek felügyelete

12.6.2 Korlátozások a szoftvertelepítésre

AzIntézmény bármely informatikai rendszerére csak az IT üzemeltető munkatársai telepíthetnek szoftvert, a felhasználónak szoftvertelepítésre és bizonyos beállítások módosítására nincs sem joga, sem lehetősége. AzIntézmény informatikai eszközeire TILOS és illegális/vagy nem jogtiszta szoftvert telepíteni! AzIntézmény informatikai struktúrájában a feladatok végrehajtására kizárólag azIntézmény által megvásárolt licenszű kereskedelmi szoftver termékeket és/vagy szabad szoftvereket lehet alkalmazni. Minden illegális, vagy nem a munkavégzést szolgáló szoftvert, adatot törölni kell a rendszerből. Ezt a műveletet a felhasználó tudtával és a CIO engedélyével az IT munkatársa végzi el.

Illegális szoftverek használata esetén a felhasználóval szemben felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárás indulhat.

A telepítést megelőzően azIntézményben vírusvédelmi célokra üzembe állított eszközzel meg kell vizsgálni a szoftver esetleges vírusfertőzöttségét. Amennyiben technikailag/technológiailag lehetséges, úgy az új szoftvercsomagról biztonsági másolatot kell készíteni. Az installálást csak a munkapéldányról szabad elvégezni. Az eredeti példányt biztonságos helyen kell tárolni.

A Intézmény infrastruktúrájában található eszközökre idegen program, adat másolása tilos!

12.7 Az információs rendszerek auditálásával kapcsolatos megfontolások

12.7.1 Az információs rendszerek auditálásával kapcsolatos intézkedések

13. A kommunikáció biztonsága

13.1 A hálózat biztonság biztosítása

13.1.1 Hálózati intézkedések

A Intézményi informatikai rendszerhez nem a saját IT infrastruktúrához tartozó informatikai kommunikációs vagy multimédiás berendezést vagy adathordozót kapcsolni tilos! Amennyiben Intézményi érdekből szükséges ilyen eszköz használata, úgy a feladat csak a Intézményvezető, vagy a CISO engedélye alapján az IT üzemeltetés bevonásával, dokumentálási kötelezettség mellet végezhető el.

13.1.2 A hálózati szolgáltatások biztonsága

13.1.3 Elkülönítés a hálózatokban

13.2 Információátvitel

13.2.1 Szabályok és eljárások az információátvitelre

13.2.2 Megállapodások az információátvitelre

13.2.3 Elektronikus üzenetküldés

Az e-mail szolgáltatás azIntézmény által a felhasználók részére biztosított eszköz. Az e-mail rendszer, valamint a rendszerben előállított, elküldött és megkapott levél is a Intézmény felügyelete alá tartozik.

A Intézmény elektronikus levelezési rendszere korlátozott mértékben, és szabályzatban rögzített feltételek betartása mellett használható személyes levelezés céljára. Az elektronikus levelező rendszer felhasználója a rendszer használatával automatikusan aláveti magát ezeknek a korlátozásnak. A Intézmény e-mail rendszerén mindennemű jogszabályellenes tartalom továbbítása és tárolása tilos.

A Intézmény nevében folytatott elektronikus levelezésre kizárólag az erre a célra biztosított elektronikus levelezési cím, a rendszeresített levelező program, illetve ezen csak a CIO által engedélyezett levelezési szolgáltatás használható. A beállítások meghatározásáért és beállításáért az IT üzemeltetési a felelős. Az elektronikus levelező rendszerben tárolt és továbbított dokumentumok elektronikus kezelésénél is be kell tartani az érvényben lévő iratkezelési és adatkezelési szabályokat.

Minden e-mail fiókkal rendelkező felhasználó köteles postaládájának tartalmát figyelemmel kísérni oly módon, hogy legalább a munkakezdéskor és a munkavégzést befejezését megelőzően meggyőződjön róla, hogy érkezett-e új üzenete, és amennyiben igen azokat kezelje (tekintse meg, tegye meg a szükséges egyéb intézkedéseket)

Az elektronikus levelező rendszer használata során nem megengedett:

- nagy mennyiségű és méretű, személyes jellegű üzenetek küldése
- kéretlen reklámok közzététele
- lánclevelek terjesztése
- a felhasználóknak a Intézményi e-mail címüket nem hivatalos minőségben használni (pl: regisztráció letöltési weboldalak, online játék oldalak)
- tilos a Intézmény nevével való visszaélés esetleges eljárási engedmények elérése érdekében
- olyan üzenetek, csatolt fájlok küldése, továbbítása, amelyek törvénytelenségeket vagy arra való felhívást tartalmaznak, fenyegetők összességében sértik a Intézmény jó hírét, általánosan elfogadott erkölcsi szabályba, vagy jogszabályba ütköznek
- a tévesen címzett, másnak szóló levelek felhasználása
- a Intézmény által biztosított e-mail címre érkező üzenetek átirányítása külső (nem a CIO által létrehozott, felügyelt és dokumentált) e-mail címre.

A levelezési rendszer személyes célokra, az elektronikus levelezésre vonatkozó szabályok betartásával, és csak akkor használható, ha az nem sérti azIntézmény érdekeit.

Az elektronikus levelek címzése során minden felhasználónak körültekintően kell eljárnia az alábbiak figyelembevételével:

- csoportos levelező, elosztási lista (pl: „mindenki", „osztály", „Intézményi dolgozók") alkalmazása során meg kell győződni arról, hogy valóban szükséges-e minden, a csoportba tartozó címzett részére elküldeni az üzenetet.
- titokvédelmi vagy egyéb biztonsági, bizalmassági okokból, amennyiben a levelek címzettjei nem szerezhetnek tudomást egymásról, vagy egymás e-mail címéről, akkor a levél „titkos másolat" („BCC": Blind Carbon Copy) kategóriáját kell alkalmazni a címzés során.

Csoportos levelező, elosztási lista létrehozása iránti igényt a szervezeti egység vezetőjének jóváhagyásával az IT üzemeltetőknek kell eljuttatni, amely a szükséges vizsgálatok, egyeztetések elvégzését követően a CISO közreműködésével dönt az igény kielégítéséről, és intézkedik annak beállítása érdekében.

A központilag létrehozott csoportos levelező, elosztási listák karbantartása az IT üzemeltetők feladata. Ennek elvégzéséhez a lista összeállítását kezdeményező szervezeti egység, illetve azIntézmény munkavállalóinak változása esetén a HR vezető köteles a CIO számára adatokat biztositani.

A postaládára vonatkozó korlátozások:

- a felhasználó postaládájának mérete korlátos, melynek méretét a CIO határozza meg a technikai lehetőségek figyelembe vételével. A meghatározottnál nagyobb postaládára vonatkozó igényt a szervezeti vezetőjének jóváhagyásával a CIO-hoz kell eljuttatni, amely a szükséges vizsgálatok, egyeztetések elvégzését követően dönt az igény kielégítéséről és intézkedik annak beállítása érdekében.

Amennyiben azIntézményi levelezésben – pontos címzés mellett – az elektronikus levelező rendszertől a kézbesítés során kézbesíthetetlenségre utaló hibajelzés érkezik, akkor a felhasználónak értesítenie kell az IT munkatársait központi elérhetőségeiken.

Az elektronikus levelek méretét, valamint a levélhez csatolt fájlok típusát az IT üzemeltető korlátozhatja a rosszindulatú kódok terjedésének megakadályozása céljából azért, hogy biztosítsa azIntézményi levelezés megfelelő szolgáltatási szintjét. A korlátozás miatt nem továbbított levelekről, csatolt fájlokról a küldő értesítést kell hogy kapjon.

Ismeretlen feladótól érkező, gyanús, csatolt fájlt tartalmazó, vagy ismeretlen linket ajánló (pl: idegen nyelvű, láthatóan reklámcélú, olyan dokumentumra hivatkozó, amiről a címzett nem tud) elektronikus üzenetek csatolmányait, illetve a kapott linkeket nem szabad megnyitni, a leveleket törölni kell.

13.2.4 Bizalmassági vagy titoktartási megállapodások

14. Rendszerek beszerzése, fejlesztése és karbantartása

AzIntézmény megfogalmazza, és azIntézményre érvényes követelmények szerint dokumentálja, valamint azIntézményen belül kihirdeti a beszerzési szabályzatot, mely azIntézmény IT rendszerére, az ezekhez kapcsolódó szolgáltatások és információbiztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg, és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő. Ezeket a szabályokat a belső minőségirányítási szabályzásban meghatározott gyakorisággal felülvizsgálja és frissíti.

17.1.3 2 Az információbiztonság folytonosságának ellenőrzése, vizsgálata és értékelése

AzIntézményi IT üzemeltetési csoport Informatikai Működésfolytonossági- és Katasztrófa Tervben leírtaknak megfelelően gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról.

17.2 Tartalékok

17.2.1 Információfeldolgozó eszközök rendelkezésre állása

18. Megfelelés

18.1. Megfelelés a jogi és szerződéses követelményeknek

18.1.1 A vonatkozó jogszabályi és szerződéses követelmények azonosítása

18.1.2 Szellemi tulajdonjogok

18.1.3 A feljegyzések védelme

18.1.4 A magántitok és a személyhez köthető információk védelme

18.1.5 A titkosítási intézkedések szabályozása

18.2 Információbiztonsági vizsgálatok

18.2.1 Az információbiztonság független vizsgálata

18.2.2 Megfelelés a biztonsági szabályoknak és szabványoknak

18.2.3 A műszaki megfelelés vizsgálata