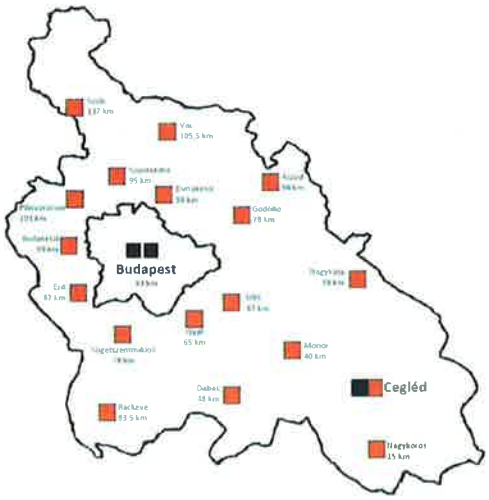
Ceglédi Tankerületi Központ

Pest Vármegyei Pedagógiai Szakszolgálat

Pest Vármegyei Pedagógia Szakszolgálat

INFORMATIKAI BIZTONSÁGRÓL SZÓLÓ BELSŐ SZABÁLYZAT



Katonáné Barna Zsuzsanna

Ceglédi Tankerületi Központ igazgató

Pinterics János

PMPSZ főigazgató

A 2011. évi CXII. törvény 27. § (5)-(7) bekezdései alapján kizárólag belső használatra készül, nem nyilvános.

Székhely: 2700 Cegléd, Ady Endre utca 3-5.

Tel.: 06/30-321-3615

E-mail: pmpsz.titkarsag@pestmszaksz.hu

Informatikai Biztonsági Szabályzata

I. ÁLTALÁNOS RENDELKEZÉSEK

1. A Szabályzat célja

1.1. Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja a Pest Vármegyei Pedagógia Szakszolgálat (a továbbiakban: PMPSZ) által használt informatikai rendszerek/alkalmazások, továbbá az informatikai rendszerek/ alkalmazások által kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, ennek érdekében az informatikai rendszerekkel/alkalmazásokkal összefüggő tevékenységekre vonatkozó szervezeti, személyi, fizikai, informatikai és adminisztratív biztonsági követelmények meghatározása, illetve ezen követelmények teljesítésével összefüggő felelősségi előírások rögzítése.

2. Az IBSZ hatálya

2.1. Az IBSZ-ben meghatározott előírás, feladat, magatartási szabály – munkakörre való tekintet nélkül – kötelező érvényű, és hatálya kiterjed:

a) a PMPSZ jogi személyiséggel rendelkező szervezeti egységeinek (a továbbiakban: köznevelési intézmények) foglalkoztatottjaira (továbbiakban: belső felhasználók);

b) a 2.1. a) pont alá nem tartozó, a PMPSZ-szel egyéb jogviszonyban álló személyek (továbbiakban: külső felhasználók), akik feladataik teljesítése során vagy egyéb céllal, jogosultsággal, vagy annak hiányában felhatalmazással, az IBSZ tárgyi hatálya alá tartozó eszközöket, szoftvereket, informatikai rendszereket használnak, adatokat vagy dokumentumokat, információkat hoznak létre, tárolnak, használnak vagy továbbítanak, valamint azokra, akik ilyen tevékenységekkel kapcsolatosan döntéseket hoznak;

az a)–b) pont alattiak a továbbiakban együtt: a felhasználók.

2.2. Az IBSZ rendelkezéseit alkalmazni kell a külső munkavégzéshez használt eszközökre is, amennyiben azok az IBSZ tárgyi hatálya alá tartoznak.

2.3. Az IBSZ-t alkalmazni kell a PMPSZ informatikai rendszereire, alkalmazásaira és azok moduljaira (a továbbiakban együtt: rendszer), az informatikai rendszerekhez csatlakoztatható informatikai, irodatechnikai, multimédiás eszközökre és adathordozókra, az informatikai rendszerekben kezelt, feldolgozott, tárolt adatokra, valamint az előzőekben felsoroltakkal kapcsolatos informatikai és biztonsági tevékenységre.

2.4. A szabályzat időbeli hatálya:

Jelen szabályzat 2024. szeptember 01-től lép hatályba és visszavonásig érvényes.

3. A Szabályzat jogi háttere és kapcsolódó belső irányítási eszközök

3.1. Az IBSZ jogi alapját az alábbi jogszabályok, közjogi szervezetszabályozó eszközök és belső irányítási eszközök képezik:

a) **2013. évi L. törvény** (a továbbiakban: Ibtv.) az állami és önkormányzati szervek elektronikus információ biztonságáról,

b) **26/2013. (X. 21.) KIM rendelet** az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus

információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról,

c) a **PMPSZ Szervezeti és Működési Szabályzata**,
d) **2011. évi CXII. törvény** az Információs önrendelkezési jogról és az információ szabadságról (továbbiakban: Iöjtv.)
e) **187/2015. (VII. 13.) Korm. rendelet** az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról,
f) **185/2015. (VII. 13.) Korm. rendelet** a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól
g) **41/2015. (VII. 15.) BM rendelet** az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
h) **2011. évi CXII. törvény** az információs önrendelkezési jogról és az információszabadságról

4. Értelmező rendelkezések

4.1. Az IBSZ-ben alkalmazott, az IBSZ értelmezését, továbbá az informatikai biztonság tárgykörét érintő informatikai fogalmak az Ibtv. figyelembe vételével:

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

Adatállomány: egy nyilvántartásban kezelt adatok összessége.

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

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

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

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

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

Adatátvitel: elektronikus adatok informatikai rendszerek közötti továbbítása, amely lehet párbeszédre épülő (online) vagy nem párbeszédre épülő (offline) elektronikus kapcsolat.

Adatbázis: azonos minőségű (jellemzőjű), többnyire strukturált adatok összessége, amelyet a tárolására, lekérdezésére és szerkesztésére alkalmas szoftvereszköz kezel.

Adatfeldolgozás: az adatkezeléshez kapcsolódó technikai feladatok elvégzése.

Adatgazda: az a vezető, aki egy meghatározott adatcsoport tekintetében az adatok fogadásában, tárolásában, feldolgozásában, vagy továbbításában érintett szervezeti egységet képviseli és az adott adatcsoport felhasználásának kérdéseiben (például felhasználói jogosultságok engedélyezésében vagy megvonásában) elsődleges döntési jogkörrel rendelkezik.

Adathordozó: az elektronikus adatkezelő rendszerhez csatlakoztatható vagy abba beépített olyan eszköz, amelynek segítségével az elektronikus adatok tárolása, terjesztése megvalósítható. Pl. CD, DAT, DVD, okostelefon, USB-memória, cloud (felhő).

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása.

Adatvédelmi incidens: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

Adminisztratív biztonsági követelmények: az informatikai rendszer használata, üzemeltetése vagy fejlesztése során az adatok és a munkafolyamatok nyilvántartását, nyomon követhetőségét, továbbá az ezzel kapcsolatos feladatok ellátásának ellenőrzését lehetővé tevő segédletek és eljárásrendek meglétére, alkalmazására vonatkozó elvárások. Pl. naplók, nyilvántartások vezetése, ellenőrzése, ennek rendje.

Archiválás: a ritkán használt, meghaladottá vált, de nem selejtezhető adatok, adatbázisrészek változatlan tartalmi formában történő hosszú távú megőrzése.

Autentikáció (azonosítás): informatikai eljárás, amelynek során a felhasználó az informatikai rendszerben az autorizáció megszerzése érdekében igazolja személyazonosságát. Lehet tudás alapú (pl. jelszavas), birtoklás alapú (pl. tokenes) vagy tulajdonság alapú (pl. biometrikus), illetve ezek kombinációi.

Autorizáció (feljogosítás): azonosításra épülő informatikai eljárás, amelynek eredményeként egyértelműen azonosított személy (eszköz) a feladatai ellátásához meghatározott hozzáférési, eljárási vagy egyéb jogosultságokat kap.

Belső felhasználó: a PMPSZ központi szerve és a PMPSZ tankerületei valamennyi foglalkoztatottja.

Belső hálózat (intranet): a PMPSZ saját, védett hálózata, elérhetővé teszi a PMPSZ feladataival összefüggő dokumentumokat, PMPSZ belső utasításokat és nyomtatványokat.

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

Biztonság: egy adott infrastruktúra, infrastruktúra elem, vagy elemek olyan – az érintett számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Részei a fizikai, környezeti, személyi, szervezeti, valamint az információbiztonság, az infokommunikációs infrastruktúrákban kezelt elektronikus adatok és információk biztonsága

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

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

Biztonsági intézkedések: illetéktelen személyek információs infrastruktúrához, vagy információkhoz való szándékos, vagy véletlen fizikai hozzáférése elleni eszközök használatát szabályozó, valamint az illetékes személyek jogosulatlan tevékenységével szemben fellépő előírások, tervek és útmutatások összessége.

Biztonsági kockázat: az informatikai rendszerrel szembeni fenyegetés, amely a rendszer rendeltetésszerű működését és/vagy a rendszerben kezelt adatok bizalmasságát, rendelkezésre állását, sértetlenségét veszélyezteti vagy veszélyeztetheti.

Biztonsági követelmények: a kockázatelemzés eredményeként megállapított, elfogadhatatlan mértékű veszély mérséklésére, vagy megszüntetésére irányuló szükségletek együttese.

Biztonsági megfelelőség: az informatikai rendszer mennyiben, milyen mértékben felel meg az informatikai biztonsági követelményeknek.

Biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége.
Biztonsági szint: a szervezet felkészültsége az Ibtv.-ben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

Elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök, eljárások, valamint az ezeket kezelő személyek együttese, továbbá az azonos adatkezelő és adatfeldolgozó által, egymással kapcsolatban álló eszközökön, egymással összefüggő eljárásokkal azonos célból kezelt, kiszolgált, illetve felhasznált adatok, az ezek kezelésére használt eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és felhasználó személyek együttese.

Elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

Értékelés: az infokommunikációs rendszerekkel kapcsolatos biztonsági intézkedések, eljárásrendek, Magyarországon elfogadott technológiai értékelési szabványok, követelményrendszerek és ajánlások, illetve jogszabályok szerinti megfelelőségi vizsgálata.

Érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy.

Észlelés: a biztonsági esemény bekövetkezésének felismerése

Felhasználók: a 2.1. pontban meghatározott személyek (egy adott elektronikus információs rendszert igénybe vevők köre).

Fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

Fizikai biztonság: illetéktelen személyek információs infrastruktúrához, vagy információkhoz való szándékos, vagy véletlen fizikai hozzáférése elleni intézkedések összessége, valamint az illetéktelen személyek, vagy illetékes személyek jogosulatlan tevékenységével szemben az adott struktúrák ellenálló képességét növelő tervek és útmutatások összessége.

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

Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.

Funkcionális rendszer: a PMPSZ működését támogató informatikai rendszer vagy alkalmazás.

Hardver: az informatikai rendszer vagy számítógép fizikai elemei

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely nem azonos az érintettel és a belső felhasználókkal.

Hálózat: számítógépek és hozzájuk kapcsolódó eszközök meghatározott szabályok szerinti összekapcsolása, amely adat- és információcserét tesz lehetővé.

Helyreállítás: valamilyen behatás következtében megsérült, eredeti funkcióját ellátni képtelen, vagy ellátni csak részben képes infrastruktúra-elem eredeti állapotának és működőképességének biztosítása, eredeti helyen.

Hozzáférés: az infokommunikációs rendszer, vagy rendszerelem használója számára a rendszer szolgáltatásainak, vagy a szolgáltatások egy részének ellenőrzött és szabályozott biztosítása.

Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

Illetéktelen személy: olyan személy, aki az adathoz, információhoz, az informatikai infrastruktúrához való hozzáférésre nem jogosult.

Infokommunikáció: az informatika és a telekommunikáció, mint konvergáló területek együttes neve.

Informatikai alkalmazás: számítógépen, illetve egyéb informatikai eszközön futó program.

Informatikai biztonság: az informatikai rendszer olyan állapota, amikor a rendszer rendeltetésszerűen működik és a rendszerben kezelt adatok bizalmassága, rendelkezésre állása, sértetlensége biztosított.

Informatikai biztonsági megbízott:

- Részt vesz a biztonsággal kapcsolatos vezetői döntések előkészítésében, kivizsgálja az informatikai rendkívüli eseményeket, elvégzi a rendszeres biztonsági ellenőrzéseket, és hatáskörében intézkedik, vagy javaslatot tesz a hibák kijavítására. Munkája során szorosan együttműködik a biztonság megvalósításában résztvevő informatikai és egyéb szakemberekkel.
- Gondoskodik az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről.
- Jóváhagyásra előkészíti az informatikai biztonsági ellenőrzési tervet és az IBSZ javításait.
- Összehangolja a biztonságot meghatározó, befolyásoló területek tevékenységét az informatikai biztonság érdekében.
- A Főigazgatóval együttműködve felügyeli a biztonsággal kapcsolatban készítendő tervek és szabályzatok elkészítését.
- Az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja, javaslatot tesz a szervezet vezetőjének a további intézkedésekre, a felelősségre vonásra.
- Az SZMSZ rendelkezései és a munkaköri leírások alapján ellenőrzi az informatikai rendszer szereplőinek jogosultsági szintjét és szükség esetén módosításukra javaslatot tesz. ***(SZMSZ-ben szabályozni kell az informatikai rendszerek, eszközök felhasználói jogosultságait – elelektronikus levelezés, INYR, KIR_SZ, KRÉTA, stb) 1. sz. melléklet***
- Ellenőrzi: az egyes felhasználói gépek hardverkonfigurációját, és a telepített szoftvereket összeveti a felhasználónak engedélyezett szoftverek listájával, hogy a rendszerben aktuálisan beállított felhasználói jogosultságok megegyeznek-e a jóváhagyott (a jogosultsági nyilvántartásban is szereplő) jogosultságokkal.
- Ellenőrzi, hogy a javításra. illetve selejtezésre kiszállított adathordozó, informatikai eszközökön adat ne kerüljön ki.
- Ellenőrzi az informatikai biztonsági követelményeket.

Informatikai biztonsági incidens: az informatikai rendszerrel szemben olyan külső, vagy belső előre tervezett, szándékos károkozású, vagy nem szándékos cselekmény, melynek célja a PMPSZ kezelésében lévő adatok, dokumentumok és egyéb információk jogosulatlan megismerése, megszerzése, módosítása valamint további károkozással kapcsolatos felhasználása.

Informatikai biztonsági követelmények: az informatikai rendszer használatával, üzemeltetésével és fejlesztésével kapcsolatos elvárások. Részterületei: a számítógépes biztonság, a kommunikációs biztonság, a kisugárzás biztonság és a rejtjelbiztonság.

Informatikai infrastruktúra: a PMPSZ-hez kapcsolódó feladatokat ellátó, illetve a PMPSZ működését biztosító hálózatba kapcsolt hardverelemek, az azokon futó szoftverek és a rajtuk megtalálható adatok együttese, amely jól körülhatárolható, önmagában is működőképes, önálló szolgáltatás nyújtására képes infrastruktúra elemekből áll.

Informatikai rendszer: a számítógépek és a hozzájuk kapcsolódó eszközök (hálózat), a számítógépeken futó programok, valamint a számítógépeken kezelt, feldolgozott adatok együttese.

Informatikai vészhelyzet: a PMPSZ információs infrastruktúrájának leállása, szolgáltatások megszakadása, elérhetetlensége, a tárolt adatok jelentős mértékű sérülése, illetve az ezekkel fenyegető rendellenes működés.

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

Információbiztonság: az adatok és információk szándékosan, vagy gondatlanul történő jogosulatlan gyűjtése, károsítása, közlése, manipulálása, módosítása, elvesztése, felhasználása, illetve természeti vagy technológiai katasztrófák elleni védelmének koncepciói, technikái, technikai, illetve adminisztratív intézkedései. Az információbiztonság része az informatikai biztonság is, melynek alapelvei a bizalmasság, sértetlenség, rendelkezésre állás.

Információvédelem: szervezeti, személyi, fizikai, informatikai és adminisztratív előírások kidolgozása és intézkedések végrehajtása az információbiztonság érdekében.

Jogosultság: az arra felhatalmazott által adott hozzáférési lehetőség valamely információs infrastruktúrához.

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

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

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

Következmény: valamely esemény, baleset, beavatkozás, vagy támadás hatása, amely tükrözi a belőle eredő veszteséget, valamint a hatás jellegét, szintjét és időtartamát.

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Kritikus adat: a személyes adat vagy valamely jogszabállyal védett adat

Különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

Külső felhasználó: a PMPSZ-kel szerződéses jogviszonyban álló magánszemélyek, jogi személyek és jogi személyiséggel nem rendelkező egyéb szervezetek és ezek alkalmazottai.

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

Mentés (biztonsági mentés): biztonsági másolat készítése az informatikai rendszerben tárolt adatokról, adatállományokról, illetve az informatikai rendszerben használt

alkalmazásokról. A másolat célja az elsődleges adattároló megsérülése esetén az adatok helyreállíthatóságának biztosítása.

Mobil eszköz: asztali munkaállomásnak nem minősülő egyes informatikai és kommunikációs feladatok ellátására használható, operációs rendszerrel, kommunikációs szolgáltatásokkal rendelkező, hordozható elektronikus eszköz. Ide tartoznak: laptopok, notebookok, táblagépek, mobiltelefonok és okostelefonok.

Munkaállomás: a felhasználó számára biztosított számítógép; lehet asztali vagy hordozható (laptop, notebook).

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

Naplózás: az informatikai rendszerben bekövetkező események, felhasználói tevékenységek és ezek időpontjának automatikus rögzítése a változások észlelése és a számon kérhetőség biztosítása érdekében.

Program: számítógépes nyelven megírt utasítássorozat. Állhat egyetlen programmodulból vagy programmodulok halmazából.

Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

Rendszerelem: információs infrastruktúra elem.

Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

Sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

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

Sebezhetőség: olyan fizikai tulajdonság, vagy működési jellemző, amely az adott információs infrastrukturális elemet egy adott veszéllyel szemben érzékennyé vagy kihasználhatóvá teszi.

Személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés.

Személyi biztonság: az adott rendszerrel/erőforrással kapcsolatba kerülő személyekre vonatkozó, alapvetően a hozzáférést, annak lehetőségeit és módjait szabályozó biztonsági szabályok és intézkedések összessége a kapcsolat felvétel tervezésétől, annak kivitelezésén keresztül a kapcsolat befejezéséig, valamint a kapcsolat folyamán a személy birtokába került információk vonatkozásában.

Szervezeti biztonság: egy adott szervezet strukturális felépítéséből adódó biztonsága és bevezetett biztonsági szabályainak és intézkedéseinek összessége a védendő rendszerhez/erőforráshoz való hozzáférés védelme érdekében.

Szoftver: a számítógép, az informatikai rendszer logikai elemei; a működtető programok (rendszerprogramok, operációs rendszerek) és a felhasználói programok (alkalmazások) összefoglaló neve.

Teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.

Tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

Titkosítás: az informatikai rendszerben kezelt adatok bizalmasságának biztosítására szolgáló, nem a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet hatálya alá tartozó olyan tevékenység vagy eljárás, amelynek során az adatot úgy alakítják át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon, de a megismerésre jogosultak számára az adat az eredeti formájába visszaállítható legyen.

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

Védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés.

Veszély (fenyegetés): természeti vagy mesterséges esemény, személy, szervezet vagy tevékenység, amely potenciálisan káros a jelen szabályzatban védett tárgyakra.

Védelem: a biztonság megteremtésére fenntartására, fejlesztésére tett intézkedések, amelyek lehetnek elhárító, megelőző, ellenálló képességet fokozó tevékenységek, vagy támadás, veszély, fenyegetés által bekövetkező kár kockázatának csökkentésére tett intézkedések.

Visszaállítás: az eredeti infokommunikációs rendszer kiesése esetén a szolgáltatások további biztosítása, korábbi mentésből való visszaállítása.

II. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETI STRUKTÚRÁJA, FELELŐSSÉGI KÖRÖK

5. PMPSZ főigazgatójának, helyetteseinek, tagintézmény-igazgatóinak és helyetteseinek feladatai

5.1. Felügyeli az informatikai biztonsági feladatok ellátását, felelős azok betartásáért.

5.2. Felelős a PMPSZ informatikai tevékenységének jogszerűségéért, beleértve az informatikai biztonsági tevékenységet is.

5.3. Kivizsgáltatja az ellenőrzések során feltárt hiányosságokat, gondoskodik a jogszabálysértő körülmények megszüntetéséről.

6. Felhasználók

6.1. Általános felhasználók a PMPSZ foglalkoztatottja.

6.2. Külső felhasználók. A PMPSZ igénybe vehet állományába nem tartozó külső felhasználókat általános, vagy kiemelt felhasználói jogosultságokkal időszakos, illetve folyamatos feladatok végrehajtására.

III. INFORMATIKAI BIZTONSÁGRA VONATKOZÓ FŐBB SZABÁLYOK

7. A felhasználókra vonatkozó szabályok

7.1. A PMPSZ-ben valamennyi felhasználó – jogosultságtól és állományba tartozástól függetlenül –:

a) felelős az általa használt, az IBSZ hatálya alá eső eszközök rendeltetésszerű használatáért,
b) a rá vonatkozó szabályok – elsősorban a PMPSZ-szel fennálló munkavégzésre, foglalkoztatásra irányuló jogviszonyt szabályozó jogszabályi rendelkezésekben foglaltak szabálytalanságokért, valamint a keletkező károkért és hátrányért, különös tekintettel az informatikai biztonsági incidens fogalomkörébe tartozó cselekményekért, – szerint felelős,
c) köteles az IBSZ-ben megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni,
d) köteles a számára szervezett informatikai biztonsági oktatáson részt venni,
e) köteles a rendelkezésére bocsátott számítástechnikai eszközöket megóvni,
f) köteles a belépési jelszavát biztonságosan kezelni,
g) felügyelet nélkül a munkahelyen (munkaállomáson) személyes adatot vagy minősített adatot tartalmazó dokumentumot, adathordozót nem hagyhat,
h) a számítógépét (a munkahelyi munkaállomást) a helyiség elhagyása esetén zárolni köteles oly módon, hogy ahhoz csak jelszó vagy hardveres azonosító eszköz használatával lehessen hozzáférni,
i) információ biztonságot érintő esemény gyanúja esetén az észlelt rendellenességekről köteles tájékoztatni a közvetlen felettesét és elektronikus információs rendszer biztonságáért felelős személyt,

j) köteles a folyó munka során nem használt hivatalos adatokat, dokumentumokat, nem nyilvános anyagokat, adathordozókat elzárni,
k) köteles a munkahelyről történő eltávozáskor az addig használt – kivéve, ha ez a rendszer(ek) más által történő használatát, vagy a karbantartást akadályozza – eszközt szabályszerűen leállítani,
l) az elektronikus levelezés és az internet használat során tartózkodik a biztonság szempontjából kockázatos tevékenységektől.

7.2. A PMPSZ informatikai rendszerét használó valamennyi felhasználónak tilos:
a) az általa használt eszközök biztonsági beállításait megváltoztatni,
b) a munkaállomására telepített aktív vírusvédelmet kikapcsolni,
c) belépési jelszavát (jelszavait), hardveres azonosító eszközét más személy rendelkezésére bocsátani, hozzáférhetővé tenni,
d) más szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő, vagy egyéb személyhez fűződő jogát vagy jogos érdekét sértő dokumentumokat, tartalmakat (zenéket, filmeket, stb.) az eszközökön tárolni, oda le-, illetve onnan a hálózatra feltölteni,

7.3. A felhasználó dokumentum nyomtatásakor köteles biztosítani, hogy az általa kinyomtatott irathoz illetéktelen személy ne férjen hozzá.

7.4. A felhasználó a rendelkezésére bocsátott, hordozható informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.

8. PMPSZ főigazgatójára, helyetteseire, tagintézmény-igazgatóira és helyetteseire vonatkozó szabályok

8.1. A PMPSZ szervezeti egységeinek vezetői (a továbbiakban: vezetők) jogosultak és kötelesek meghatározni az irányításuk alá tartozó foglalkoztatottak munkavégzéséhez szükséges:
a) informatikai, irodatechnikai, multimédiás és kommunikációs eszközök körét,
b) a használandó informatikai rendszerek és az ahhoz szükséges jogosultságok körét.

8.2. A PMPSZ szervezeti egységének vezetői kötelesek együttműködni az elektronikus információs rendszer biztonságáért felelős személlyel annak informatikai biztonsági feladatai ellátása során.

8.3. A vezetők jogosultak és kötelesek az informatikai eszközök munkavégzéshez szükséges használatának biztosítása érdekében a szükséges informatikai eszköz és jogosultság igénylési eljárásokat kezdeményezni a PMPSZ informatikáért felelős szervezeti egysége felé.

8.4. A vezetők kötelesek gondoskodni az irányításuk alá tartozó foglalkoztatottak informatikai biztonsági ismereteinek naprakészen tartásáról, beleértve az IBSZ és az IBSZ-el kapcsolatos PMPSZ rendelkezések szükséges mértékű ismeretét is.

9. Külső felhasználókra vonatkozó szabályok

9.1. A PMPSZ informatikai rendszereihez és eszközeihez külső felhasználó csak érvényes szerződés alapján, dokumentáltan férhet hozzá.

9.2. A PMPSZ informatikai rendszereihez és eszközeihez hozzáférő külső felhasználó egyedileg köteles nyilatkozatot tenni arról, hogy az IBSZ-ben foglaltakat megismerte és az abban foglaltakat magára nézve kötelezőnek ismeri el.

9.3. A PMPSZ informatikai rendszereihez és eszközeihez hozzáférést biztosító szerződés csak olyan külső felhasználóval köthető, aki/amely az IBSZ-ben foglaltakat magára nézve kötelezőnek ismeri el.

IV. INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK

10. Biztonsági követelmények

10.1. Az informatikai eszközöket úgy kell telepíteni és tárolni, hogy azokhoz a foglalkoztatottakon, külső felhasználókon kívüli más személy hozzáférése kizárt legyen.

10.2. A PMPSZ tulajdonát képező vagy az általa használt informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót a PMPSZ objektumaiból kivinni csak hivatali feladat ellátására, a közvetlen vezető elektronikus írásbeli engedélyével lehet.

10.3. Az informatikai rendszerekben csak jogtiszta szoftver telepíthető.

10.4. A PMPSZ területén a PMPSZ által kezelt adatok védelmére vonatkozó rendelkezéseket vagy személyiségi jogokat sértő, továbbá a PMPSZ működésére vonatkozó magáncélú adatrögzítés – beleértve a hang- és képfelvétel készítését is – tilos.

10.5. Az elektronikus adatokat tároló eszközöket a rajtuk tárolt vagy tárolandó adatokat a jogszabályi előírásoknak megfelelően kell kezelni.

10.6. Az elektronikus adatokat tároló eszközök azonosítását, mozgásuk nyomon követhetőségét az átadás-átvétel, továbbítás, selejtezés, megsemmisítés dokumentálásával biztosítani kell.

10.7. Az elektronikus adathordozók kezelése vonatkozásában az IBSZ-ben nem szabályozott kérdésekben az Iratkezelési Szabályzat előírásai értelemszerűen irányadóak.

10.8. A papír alapú dokumentumok előállítására alkalmas eszközök (nyomtató, fax) használatára az informatikai eszközökre vonatkozó szabályozások érvényesek. A felhasználók számára tiltott tevékenységek a PMPSZ adatait nyomtatott formában megjelenítő eszközök esetén is irányadóak.

11. Működtetési követelmények

11.1. A fenyegetettségek elemzését és a kockázatok meghatározását az elektronikus információs rendszer biztonságáért felelős személy hajtja végre, szükség szerint független külső szakértő bevonásával.

11.2. Amennyiben az IBSZ rendkívüli módosítása szükséges – a szükséges módosítás jellegétől vagy terjedelmétől függetlenül – az információs rendszer biztonságáért felelős személy közvetlenül jelzi ezt a PMPSZ vezetőjének.

11.3. Minden felhasználó kötelessége – amennyiben kellő gondossággal eljárva azt felismerhette – a lehetséges legrövidebb időn belül közvetlen vezetőjén keresztül bejelenteni az elektronikus információs rendszer biztonságáért felelős személy részére minden olyan veszélyforrást, amely az elektronikus információbiztonságra nézve érdemi fenyegetést jelent vagy jelenthet.

11.4. A biztonsági eseményeket soron kívül ki kell vizsgálni. A vizsgálatot az elektronikus információs rendszer biztonságáért felelős személy folytatja le

11.5. A vizsgálat eredményét az elektronikus információs rendszer biztonságáért felelős személy írásban dokumentálja

11.6. Az informatikai biztonsággal kapcsolatos szabályok megszegése esetén a szabályszegőkkel szemben érvényesítendő jogkövetkezmények tekintetében elsősorban annak súlyosságára tekintettel vagy etikai, vagy munkáltatói fegyelmi jogkörben kell eljárni.

11.7. Az információbiztonsággal kapcsolatos szabályok súlyos megszegése vagy annak gyanúja esetén az elektronikus információs rendszer biztonságáért felelős személy javaslatára – érintett foglalkoztatott közvetlen vezetője, illetve az utasítási joggal rendelkező vezető véleményének kikérésével – a főigazgató jogosult a megfelelő jogkövetkezmények érvényesítése érdekében eljárást indítani, illetőleg eljárás megindítását kezdeményezni.

11.8. A felhasználó az informatikai rendszert csak egyértelmű azonosítást követően, a számára meghatározott és biztosított jogosultságok keretei között használhatja.

11.9. Minden felhasználót kizárólagos személyi használatú egyedi azonosítóval kell ellátni, amelyhez minimálisan egyedi jelszót kell rendelni. További azonosítási lehetőségek is elfogadottak, melyek az elektronikus információs rendszer biztonságáért felelős személy engedélyével vezethetők be.

11.10. A felhasználói jelszónak legalább az alábbi követelményeket teljesítenie kell:

a) legalább 6 karakter hosszú,
b) kis- és nagybetűket és számokat vegyesen tartalmaz,
c) nem tartalmazhat könnyen kitalálható, ismétlődő karaktersorozatot,
d) nem utalhat a felhasználó személyére,
e) érvényességi ideje legfeljebb 90 nap,
f) az utolsó négy jelszó használata tiltott
g) maximum 5 téves próbálkozás után a fiók/munkaállomás zárolási ideje 15 perc.

11.11. A felhasználó köteles a jelszót bizalmasan őrizni, illetéktelenek általi megismerését kizárni.

11.12. Tilos a jelszót más által megismerhető módon feljegyezni, azt mással bármilyen formában közölni.

11.13. A hálózathoz csatlakozó munkaállomásra csak a munkavégzéshez szükséges adatállományok, programok tölthetők le, illetve telepíthetők.

11.14. A hálózathoz csatlakozó munkaállomásra nem telepíthető, nem másolható – ideiglenesen sem –, illetve a belső hálózaton nem tehető közzé olyan adatállomány, információ, amely

a) jogszabályt sért, így különösen adatvédelmi, szerzői jogvédelmi, személyiségvédelmi előírásba ütközik,
b) a hálózat rendeltetésszerű működését, biztonságát veszélyezteti vagy veszélyeztetheti, így különösen annak erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon veszi igénybe.

11.15. Az internet felhasználása csak a PMPSZ ügymenete érdekének megfelelően kialakított és betartott szabályok alapján történhet.

11.16. Felhasználók internet használatára vonatkozó általános szabályok:

a) csak a munkavégzéshez, szakmai tájékozottság bővítéséhez szükséges vagy általános tájékozottságot biztosító információt, segítséget nyújtó oldalak látogathatók,
b) tilos a jó ízlést, közerkölcsöt sértő, rasszista, uszító és más, a véleménynyilvánítás kereteit meghaladó oldalak szándékos látogatása, online játékok, fogadási oldalak felkeresése, bármely tartalommal kapcsolatos magánvélemény kinyilvánítása (pl. privát blog és chat),
c) a felhasználók nem tölthetnek fel egyénileg – a felelős jóváhagyása nélkül – a PMPSZ-val kapcsolatos adatot az internetre,
d) az internetről csak a munkavégzéshez szükséges adatállományok, táblázatok, tölthetők le, alkalmazások, programok nem,
e) a látogatott oldal nem szokványos működése (pl.: folyamatos újratöltődés, kilépés megtagadása, ismeretlen oldalak látogatására történő kényszerítés, ismeretlen program futásának észlelése, stb.) esetén a közvetlen technikai támogató segítségét kell kérni.

11.17. A PMPSZ feladatainak végrehajtásához alkalmazott elektronikus levelezésben kizárólag az intézményi gmail.com végződésű, hivatali levelezési cím használható.

A PMPSZ tevékenységével össze nem függő célra a hivatali postafiók, levelezési cím nem használható.

11.18. A levelezőrendszerek használata során a vírusvédelmi előírásokat folyamatosan érvényesíteni kell.

11.19. A hivatali levelezőrendszeren kizárólag hivatali célú üzenetek továbbíthatók. Magáncélú üzenetet nem nevesített felhasználóknak (pl. csoport, mindenki) küldeni tilos.

11.20. A távoli segítségnyújtás (távsegítség) során a kliensoldali programot, amely bármilyen módon lehetővé teszi a felhasználó képernyőjén lévő információk távoli elérését vagy input eszközeinek távvezérlését, csak a felhasználó indíthatja el, azt automatikusan induló programként telepíteni tilos. A távsegítség bevezetése és alkalmazása előtt a szolgáltatás

tartalmáról, továbbá a távsegítség során elvégzett beavatkozásról a felhasználókat tájékoztatni kell.

11.21. Az informatikai rendszerekben kezelt és tárolt adatok rendelkezésre állását rendszeres és indokolt esetben soron kívüli mentéssel kell biztosítani.

11.22. Az informatikai rendszerekben kezelt adatállományokat, amennyiben azok elérése a felhasználók számára napi munkavégzésük során nem szükséges, azonban őrzésük indokolt, archiválni kell.

11.23. A vírusvédelmi eljárásokat, a vírusvédelemre vonatkozó szabályozást, beleértve az intézkedési rendet, úgy kell kialakítani, hogy az

a) a folyamatos vírusvédelmi felügyelet ellátását lehetővé tegye,
b) támogassa a valós riasztások kiszűrését,
c) alkalmas legyen a súlyos gondatlanságot, szándékosságot jelentő esetek felismerésére,
d) tegye lehetővé az általános vírusbiztonsági helyzet értékelését,
e) biztosítsa az új fenyegetések időben történő felismerését.

11.24. A hálózat esetében a vírusvédelem központilag biztosított.

11.25. A vírusvédelmi előírások súlyos, szándékos vagy sorozatos megsértése rendkívüli információbiztonsági eseménynek(incidens) minősül.

V. INFORMÁCIÓBIZTONSÁGI ELJÁRÁSOK

12. Általános irányelvek

12.1. Az azonosítók képzését, azok nyilvántartását, a jogosultságok kezelését a FIRSTEP Kft. végzi.

12.2. Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör, feladat ellátásához szükséges minimális funkcióelérést biztosíthatják.

12.3. A felhasználók a hozzáférésüket megalapozó jogviszonyuk létrejöttét követően (a lehető legrövidebb időn belül) megkapják felhasználói azonosítójukat.

13. Munkaállomások hozzáférésére vonatkozó minimális előírások

13.1. A számítógépes munkaállomások képernyőit (monitor) úgy kell elhelyezni, hogy az azon megjelenő információkat illetéktelen személy ne láthassa.

13.2. A munkaállomás beállításait adminisztrátori jelszóval kell védeni módosítás ellen.

13.3. A képernyőt automatikus védelemmel kell ellátni (munkaállomás zárolás).

14. Szoftvereszközök használatának szabályozása

14.1. Az informatikai biztonság teljes körű megvalósításához hozzájárul a jogtiszta szoftverek és a szoftvereszközök jogszerű használata, valamint a szoftverek biztonságos kezelése.

14.2 a felhasználók rendelkezésére bocsátott hardver és szoftver eszközök ellenőrzését az elektronikus információs rendszer biztonságáért felelős személy bejelentés nélkül bármikor kezdeményezheti.

15. Távoli hozzáférés szabályozása

15.1. A PMPSZ informatikai rendszerének távoli elérésére csak egyedileg azonosított felhasználók számára lehetséges.

15.2. A PMPSZ informatikai környezetében jelenleg az alábbi pontokban feltüntetett szolgáltatások sorolhatók távoli elérés alá:

a) Távsegítség nyújtása (Kizárólag rendszergazdák)
b) NetStat SQL adatbázis elérés (Kizárólag NetStat felhasználók)

16. Adatvédelmi incidens

Adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítés, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Felügyeleti hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság

16.1 Az adatvédelmet sértő esemény észlelése, feltárása, bejelentése

16.1.1. Adatvédelmi incidens bekövetkezése esetében az ezt észlelő munkavállaló haladéktalanul, de legkésőbb annak észlelésétől számított 24 órán belül köteles jelezni az incidenst e-mailben a következő címre: pmpsz.titkarsag@pestmszaksz.hu, vagy telefonon (+36 30 321 3615) az adatkezelőnek.

16.1.2. Az incidenst az adatkezelő haladéktalanul, az adatvédelmi tisztviselő bevonásával kivizsgálja abból a szempontból, hogy az valószínűsíthetően jár-e kockázattal a természetes személyek jogaira és szabadságaira nézve.

16.1.3 Amennyiben a kivizsgálás eredménye alapján az incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, legkésőbb 72 órával az incidens észlelését követően az adatkezelő elektronikus úton, a GDPR 33. cikk (3) bekezdése szerinti tartalommal bejelenti az incidenst a felügyeleti hatóságnak és az incidens kezelése érdekében megteszi a szükséges technikai, illetve szervezeti intézkedést.

16.1.4. Amennyiben a kivizsgálás eredménye alapján az incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintett(ek)et az incidensről, kivéve, ha a GDPR 34. cikk (3) bekezdésében meghatározott feltételek bármelyike fennáll.

Adatvédelmi incidens nyilvántartás lsd, 2. sz. mellékelt

VI. ELLENŐRZÉSEK, RENDSZERES FELÜLVIZSGÁLATOK

17. Ellenőrzésekre vonatkozó szabályok

17.1. Az informatikai biztonsággal kapcsolatos ellenőrzések területei az alábbiak lehetnek:

a) információbiztonság szintjére vonatkozó vizsgálat – célja felderíteni, hogy az információbiztonság szintje megfelel-e a meghatározott védelmi szintnek,
b) információbiztonsági szabályok betartásának ellenőrzése – célja felderíteni, hogy a PMPSZ információbiztonsági szabályait a felhasználók ismerik-e, illetve betartják-e,- ez az ellenőrzés az informatikai biztonság egy-egy területére is leszűkíthető,

17.2. Az ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

a) a mentési rendszer megfelelő alkalmazását,
b) a hozzáférési jogosultságok naprakészségét, a kiadott jogosultságok szükségességét,
c) az alkalmazott szoftverek jogtisztaságát,
d) a fizikai biztonsági előírások betartását.

Készült 2 darab eredeti példányban, kapja:

- Pest Vármegyei Pedagógiai Szakszolgálat
- Ceglédi Tankerületi Központ

1. sz. melléklet

SZINT	JOGOSULTAK	JOGOK
Minimum	Az intézmény bármely dolgozója, akinek a munkájához szükséges az informatikai eszköz használata	Általános azonosító, mely lehetővé teszi a munkához szükséges adatok elérését, Internet használata, wifi hozzáférés lehetősége.
Alap	Az intézmény bármely dolgozója, akinek a munkájához szükséges az informatikai eszköz használata	Minimum szint, továbbá Egyéni azonosító, Internet használat, saját könyvtár az intézményi/tagintézményi szerveren.
Ügyviteli, adminisztrációs	ügyviteli alkalmazottak, szakszolgálati titkárok	Alap szint, továbbá e-mail cím, elektronikus levelezés, valamint hozzáférés a munkaköre ellátásához szükséges központi tárhelyekhez.
Pedagógus	Pedagógus munkakörben dolgozók	Alap + hozzáférés a saját mappához és az adminisztrációs adatokhoz. Egyéni belépési és felhasználói jogosultságok a munkához szükséges informatikai rendszerekhez (INYR, KRÉTA)
Vezetői	Főigazgató, általános főigazgató-helyettes, koordinációs főigazgató-helyettes, szakmai főigazgató-helyettes, tagintézmény-igazgató, tagintézmény-igazgató helyettes	Alap + Ügyviteli, adminisztrációs +Pedagógus, valamint vezetői jogosultságok az informatikai rendszerekben (KIR-SZNY, INYR, KRÉTA, OKTIG, KIR-STAT)
Rendszergazda	Az adott feladatra kijelölt személy	Alap + Speciális jogok megadott feladatok elvégzéséhez (pl. a weboldalak karbantartása)

2. sz. melléklet

A Ceglédi Tankerületi Központ 4/2021. (VII. 12-) számú Adatvédelmi és adatbiztonsági szabályzatának 5. sz. melléklete

Adatvédelmi incidens nyilvántartás

(elektronikusan szükséges vezetni)

Sorszám	
Az incidens bejelentésének, vagy tudomásszerzésének időpontja:	
A NAIH felé történő bejelentés időpontja, vagy annak a jelzése, hogy nem volt szükség a Hatóság felé bejelenteni:	
A biztonságot érintő esemény körülményeinek leírása, a kapcsolódó dokumentumok meghatározása:	
Az incidens bekövetkezésének meghatározott vagy vélelmezett időpontja:	
Az adatvédelmi incidenssel érintett szervezeti egység:	
Az adatvédelmi incidens jellege:	• adathalászat • elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön) • eszköz elvesztése vagy ellopása • informatikai rendszer feltörése (hackelés) levél elvesztése vagy jogosulatlan felnyitása • papír alapú dokumentum elvesztése, ellopása, vagy olyan helyen hagyása, amely nem minősül biztonságosnak • papír alapú dokumentum nem megfelelő módon történő megsemmisítése • rosszindulatú számítógépes programok pl. zsarolóprogram • személyes adatok jogosulatlan megismerése • személyes adatok jogosulatlan szóbeli közlése • személyes adatok nagy nyilvánosság előtti jogellenes közzététele • személyes adatok téves címzett részére történő elküldése • egyéb, mégpedig:

Az adatvédelmi incidens oka:	• külső, rosszhiszemű cselekmény • külső, rosszhiszeműnek nem minősülö cselekmény • szervezeten belüli, rosszhiszemű cselekmény • belüli, rosszhiszeműnek nem minősülő cselekmény • egyéb, mégpedig:
Az incidenssel érintett személyes adatok köre:	*(Személyazonossághoz kapcsolódó adatok, személyi szám, elérhetőségi adatok, azonosító adatok, gazdasági, pénzügyi adatok, képfelvétel, hangfelvétel, hivatalos okmányok, helymeghatározó adatok stb.)*
Az incidens érintett-e különleges személyes adatokat, és ha igen, ezek köre:	(*Faji eredetre, nemzetiséghez tartozásra vonatkozó adatok, politikai véleményre vonatkozó adatok, vallásos vagy más világnézeti meggyőződésre vonatkozó adatok, érdekképviseleti szervezeti tagságra vonatkozó adatok, szexuális életre vonatkozó adatok, egészségügyi adatok, genetikai adatok stb,)* *Amennyiben még nem ismert, ennek jelölése.*
Az incidenssel érintettek köre/csoportja:	(*Alkalmazottak, felhasználók, tanulók, tanárok, szülők, ügyfelek (jelenlegi és potenciális), kiskorúak stb.)* *Amennyiben még nem ismert, ennek jelölése.*
Az incidenssel érintettek becsült vagy meghatározott száma:	
Az incidens valószínűsíthető hatásai az érintettekre:	*(érintett jogainak korlátozása, hátrányos megkülönböztetés jó hírnév sérelme, pénzügyi veszteség szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, személyazonosság-lopás, személyazonossággal való visszaélés, személyes adatok feletti rendelkezés elvesztése stb.)*
A valószínűsíthető következmények súlyossága:	• elhanyagolható • korlátozott • jelentős • maximális
Az incidens során:	• sérült a bizalmas jelleg • sérült az integritás • sérült a rendelkezésre állás • egyik sem sérült
Az incidens elhárításra tett intézkedések, ideértve a hatósági vagy fegyelmi eljárást, következményt, ennek adatai:	
Az érintettek tájékoztatása:	• megtörtént • nem történt meg

	• az adatkezelő mentesült a tájékoztatási kötelezettség alól nem volt szükség a tájékoztatásra (pl. mert az érintett maga jelentette be)
Az incidens elhárításának vagy megszűnésének időpontja, vagy ha még továbbra is fennáll. akkor ennek jelzése:	