Budapest Főváros XV. kerületi Önkormányzat
Újpalotai Összevont Óvoda

Iktatószám: 238/2020.

IT ÜZEMELTETÉS ADATVÉDELMI SZABÁLYZATA

Érvényes: 2020.06.30 - tól

TARTALOMJEGYZÉK

Dokumentum változás követése

Verzió-szám	Iktatószám (előzmény)	Dokumentum címe	Változás leírása	Felelős (beosztás)	Hatályba lépés dátuma
V_1		IT Üzemeltetés adatbiztonsági szabályzat	Alapdokumentum	Intézményvezető	2018.05.25
V_2	238/2020	IT Üzemeltetés adatbiztonsági szabályzat	Blső ellenőri megállapítások átvezetése	Intézményvezető	2020.06.30

Fogalomtár

Sorszám	Fogalom / rövidítés	Meghatározás
1.	Alkalmazás	(angol: application, app) egy számítógépes program, ami egy fordítóprogram segítségével készül el egy forráskódból. A számítógépes programok ezen elnevezése elsősorban a Windows operációs és felhasználói rendszerek magyar fordítógárdája munkája nyomán terjedt el.
2.	Anonimizálás (álnevesítés)	Az éles adatbázisban a természetes személyek minden olyan adatának véletlenszerű, de hasonló típusú adattal történő felülírása, amely alapján a természetes személyek beazonosíthatósága már nem lehetséges. Ugyanakkor az adatbázis jellege és struktúrája megmarad, és így az – esetleges – programhibák beazonosíthatósága megmarad.
3.	Intézmény	Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Újpalotai Összevont Óvoda
4.	IT BCP-DRP terv	BCP-DRP terv az információbiztonsági szakmában közismert rövidítése az üzletmenet-folytonossági és katasztrófa-elhárítási terveknek, ami rövidítés az angol megfelelőjük (Business Continuity Plan – Disaster Recovery Plan) rövidítéséből, mint mozaik betűszó adódik.
5.	Kétfaktoros azonosítás	további második azonosítási mód egyidejű alkalmazása
6.	Fájl	(Angol: File) Adatállomny
7.	Felhasználó	Aki az IT rendszereket, alkalmazásokat az eszközökön keresztül használja.
8.	GDPR	GDPR rendelet - EU Parlament és Tanács 2016/679. sz. rendelet 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)
9.	GMK	Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Gazdasági Működtetési Központ
10.	HDD	(Angol: **H**ard **D**isk **D**rive) Merevlemez
11.	IP	(Angol: **I**nternet **P**rotocol, rövidítve: IP) az internet (és internetalapú) hálózat egyik alapvető szabványa (avagy protokollja). Ezen protokoll segítségével kommunikálnak egymással az internetre kötött csomópontok (számítógépek, hálózati eszközök, webkamerák stb.). A protokoll meghatározza az egymásnak küldhető üzenetek felépítését, sorrendjét stb.

Sorszám	Fogalom / rövidítés	Meghatározás
12.	Kliens	Olyan számítógép vagy azon futó program, amelyik hozzáfér egy (távoli) szolgáltatáshoz, amelyet egy számítógép hálózathoz tartozó másik számítógép (a szerver) nyújt
13.	Operációs rendszerek	röviden **OS** az angol **O**perating **S**ystem alapján) nevezzük a számítástechnikában a számítógépeknek azt az alapprogramját, mely közvetlenül kezeli a hardvert, és egy egységes környezetet biztosít a számítógépen futtatandó alkalmazásoknak (például szövegszerkesztők, játékok stb.)
14.	Pendrive	(USB-flash-tároló, USB-kulcs, tollmeghajtó) USB-csatlakozóval egybeépített flash memória.
15.	Perifériák	A fogalmat eredetileg azokra az eszközökre alkalmazták, melyek külsőleg csatlakoztak a gazdagéphez, tipikusan egy számítógépes buszon keresztül, mint például az USB. Tipikus példa a joystick, nyomtató, és lapolvasó.
16.	RAID technológia	Minden RAID szint alapjában véve vagy az adatbiztonság növelését vagy az adatátviteli sebesség növelését szolgálja.
17.	Rendszergazda	A számítógép-hálózat, illetve a benne levő számítógépek telepítésével és karbantartásával megbízott személy.
18.	RPO	RPO (Peturn Point of Objective) az IT rendszer működésének leállása utáni visszaállításkor az az állapot, amire a rendszer vissza tud állni (gyakorlatilag maximálisan mennyi idővel lehet az utolsó elmentett állapot a leállást megelőzően)
19.	RTO	RTO (Return Time of Objective) az IT rendszer működésének leállása utáni időtartam, amin belül az IT rendszer újra üzemképessé válik (gyakorlatilag a megengedett legnagyobb leállási időtartam)
20.	NIF	Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Népegészségügyi és Intézmény Felügyeleti Főosztály
21.	Szerver	(az angol server szóból) vagy kiszolgáló az informatikában olyan (általában nagy teljesítményű) számítógépet vagy szoftvert jelent, ami más számítógépek számára a rajta tárolt vagy előállított adatok felhasználását, a szerver hardver erőforrásainak (például nyomtató, háttértárolók, processzor) kihasználását, illetve más szolgáltatások elérését teszi lehetővé.
22.	VPN	(angolul **V**irtual **P**rivate **N**etwork) egy nyilvános hálózaton keresztül kiterjeszti a helyi hálózatot.
23.	Windows	a Microsoft Corporation gyártotta operációs rendszerek, illetve az ezekbe épített többfeladatos grafikus felhasználói felületek, valamint bizonyos mobiltechnológiák családja. A „Windows" szó és logó a Microsoft cég védjegye.
24.	Wi-Fi	(WiFi, Wifi vagy wifi), az IEEE által kifejlesztett vezeték nélküli mikrohullámú kommunikációt (WLAN) megvalósító, széleskörűen elterjedt szabvány (IEEE 802.11) népszerű neve.

1. A szabályzat tárgya és kritériumai

A szabályozás tárgya: A Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Újpalotai Összevont Óvoda (továbbiakban: Intézmény) és tagóvodáiba a mindenkor hatályos GDPR és jogszabályi elírásoknak megfelelő adatkezelői és adatkezlési tevékenységgel kapcsolatos informatikai technológiai (továbbiakban: IT) üzemeltetési szabályait tartalmazza.

A szabályozás kritériumai: Az adatkezelő az adatkezelési tevékenységét úgy végzi, hogy az feleljen meg az Európai Parlament és Tanács 2016/679. számú Általános Adatvédelmi Rendeletének, (továbbiakban: a GDPR) amely alapvetően szabályozza a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását.

2. A Szabályzat célja

A jelen szabályzat **célja** az Intézmény általános működésében minden informatikai rendszerhasználat során előírni azokat az alapvető, az informatikai rendszerek biztonságos üzemeltetésére vonatkozó biztonsági szabályokat, amelyek az alapvető adatok (elsősorban a személyes adatok szempontjából történő) kezelésének adatbiztonsági feltételeit biztosítják.

Az Intézmény által kezelt személyes adatok adatbiztonságának kialakításához és fenntartásához – a jelen szabályzat előírásán, betartásán és számonkérésén túlmenően – szükség van még az informatikai infrastruktúrának az azt használó munkatársak általi biztonságos használatára is, amelyre vonatkozó adatbiztonsági alapelveket a mindenkor hatályos *Munkavállalói Adatbiztonsági szabályzat* tartalmazza.

3. A szabályzat hatálya

A jelen szabályzat **hatálya** kiterjed az Intézmény informatikai rendszerét üzemeltető rendszergazdára vagy rendszergazdai csoportra, függetlenül hogy az az Intézmény alkalmazottja vagy külső szolgáltató. (Külső szolgáltató a GMK, ezért jelen szabályzat alkalmazását az *Együttműködési megállapodáson* keresztül kell előírni, odafigyelve a jelen szabályzatban előírtak betartásának ellenőrzésére is.)

4. A szabályzat használata

Jelen adatbiztonsági szabályok azokat az általános informatikai biztonsági jellegű alapelveket foglalják össze, amelyek figyelembe vétele és betartása minimálisan szükségesek az Intézmény informatikai infrastruktúra üzemeltetése során, hogy a személyes adatok kellő adatbiztonsága biztosítható legyen.

Jelen adatbiztonsági szabályok az informatikai biztonság egyes területein csak a betartandó alapelveket mondják ki. Azok konkrét megvalósítása mindig a pillanatnyi konkrét IT infrastruktúra és üzemeltetési mód függvénye, ami többféleképp is megvalósítható. Az itt (ebben a szabályzatban) leírt alapelvek konkrét megvalósítást a rendszergazdának (GMK) a saját belső, végrehajtási előírásai kell, hogy tartalmazzák, és azok alapján kell azokat betartaniuk.

Jelen adatbiztonsági szabályok betartása csupán az általános, informatikai biztonsági gyakorlatnak megfelelő alapszintű biztonságot garantálja, egyes rendszerek nagyobb kockázata esetén azon rendszerekhez kockázati kitettség alapon egyedi, szigorúbb biztonsági intézkedések vezethetők / vezetendők be.

5. A fizikai elhelyezés és az üzemeltetés fizikai biztonsága

1. Az informatikai rendszer központi kiszolgáló elemeit (hálózati eszközök, szerver számítógépek, telekommunikációs eszközök) elkülönített, ellenőrizhető, zárt, a fizikai hozzáférést szabályozott szerverszobában kell elhelyezni. A külső szolgáltatónál (GMK-nál) működő szerverszoba esetén, a GMK belső biztonsági előírásai az irányadóak.
2. Az informatikai hálózat szerverszobán kívül elhelyezkedő hálózati elemeit (pl. switchek, routerek, hubok, AP-ok) úgy kell elhelyezni, hogy lehetőleg elzártak és nehezen hozzáférhetőek legyenek, védeni kell minden illetéktelen hozzáféréstől.
3. Személyes adatokat is tartalmazó informatikai eszközök, rendszerek karbantartását csak a rendszergazda, vagy szükség esetén a rendszergazda felügyelete mellett megfelelő szakszerviz munkatársai végezhetik, akikre a karbantartási szerződés érvényes és a Titoktartási nyilatkozatot aláírták.
4. Régi vagy meghibásodott elektronikus adathordozókat, – amelyek személyes adatokat is tartalmaz(hat)nak – kidobni, cserére átadni nem szabad, azokat fizikailag kell használhatatlanná tenni.

6. Jogosultságok menedzselése

1. A vállalat erőforrásait kizárólag a feljogosított felhasználók érhetik el.
2. A feljogosítás megfelelő felhasználónevet, jelszavat illetve a felhasználóra meghatározott jogosultságot jelent.
3. A feljogosításokat csak a szervezeti vezető engedélyezheti, a beállításokat csak a rendszergazda végezheti el.

4. A felhasználói jogosultságokat csoportszinten kell meghatározni. (Egyedi, azaz csoporton kívüli felhasználói jogosultságok kizárólag felső vezetői engedéllyel, korlátozott időre adhatók.)

5. A felhasználói csoportokhoz történő rendelés egyértelműen biztosítsa a munkakörhöz szükséges és elégséges erőforrások elérését.

6. A felhasználók a kiszolgálórendszereket számítógépeken keresztül az integrált címtárszolgáltatáson keresztül érhetik csak el, amely a számítógépek részére hitelesítési és jogosultság-kezelési szolgáltatásokkal biztosítja a hálózaton elérhető erőforrások (fájlok, megosztások, perifériák, adatbázisok, felhasználók, csoportok stb.) központosított felügyeletét.

7. Az erőforrásokhoz (szervereken megosztott mappák, nyomtatók, levelezés, informatikai alkalmazások stb.) a felhasználónkénti egyedi hozzáférés minimum felhasználónév/jelszó páros megadásával, az érzékeny, különleges személyes adatokat is tartalmazó rendszerek esetén pedig további második azonosítási mód egyidejű alkalmazásával (ún. két-faktoros authentikáció) legyen biztosított.

7. Hálózatbiztonsági szabályok

7.1. Belső hálózati szabályok

1. Az Intézmény informatikai hálózatáról, annak alkotóelemiről és működési beállításairól a rendszergazdának dokumentált nyilvántartást kell vezetnie.
2. Az Intézmény belső hálózatára csak az Intézmény saját tulajdonú leltárba vett hálózati eszközei csatlakoztathatók.
3. A hálózati eszközöknek minden esetben IP kapcsolaton keresztül menedzselhető eszközöknek kell lenniük, az eszközöknek egyedi rendszergazdai jelszóval kell rendelkezniük, melyet a rendszergazda a titkosított jelszótároló rendszerben rögzít.
4. A hálózati eszközök működését a központi monitoring rendszeren keresztül a rendszergazdának folyamatosan ellenőriznie kell.
5. Az Intézmény internet irányába történő kommunikációját tűzfalon keresztül kell kialakítani.
6. A tűzfalon a rendszergazdának szigorú, dokumentált szabályrendszert kell beállítania és fenntartania a külső támadások elhárítása, illetve a kifele indított kommunikáció felügyelete érdekében.

7.2. Intézmény Wi-Fi használati szabályai

1. Az Intézmény belső hálózatához kapcsolódó Wi-Fi hálózata:
   - hozzáférési engedély csak munkatársaknak, és csak vezetői engedéllyel adható;
   - hozzáférés csak az Intézmény tulajdonát képező, a rendszergazda által felügyelt eszközzel lehetséges;
   - kizárólag csak munkavégzés céljára használható.
2. Az Intézmény belső hálózatáshoz is kapcsolódó Wi-Fi hálózatának szigorú biztonsági beállításait a rendszergazda menedzseli, és szükség szerint aktualizálja.
3. Vendégek számára internet elérés, illetve munkatársak számára saját mobil eszközön keresztüli internetezés céljára csak külön ún. vendég- Wi-Fi hálózat engedélyezhető, amelyről az Intézmény belső hálózata elérése tiltott, nem lehetséges.
4. A Vendég Wi-Fi hálózatot is jelszóval, és minimum WPA2 titkosítással kell védeni.

7.3. Távmunka és otthoni munkavégzés

1. Távmunka illetve az otthoni munkavégzés csak az intézményvezető dokumentált engedélyével lehetséges.
2. A vállalat belső hálózatára való távoli csatlakozás:
   - csak a felhasználó egyéni jogosultságával (accountjával) engedélyezett, amit a rendszergazda állít be számára, és amit a felhasználó senki másnak nem adhat át;
   - csak biztonságos VPN kapcsolaton keresztül lehetséges, amelyet a rendszergazda állított be és felügyel;
   - csak olyan munkaállomásról engedélyezett, amelyhez a felhasználó a megfelelő védelmet (biztonsági csomagok telepítve vannak, elégséges vírusvédelem, hardveres tűzfal/router kapcsolódási pont) folyamatosan biztosítja.
3. Személyes adatokat is tartalmazó rendszerekhez, eszközökhöz való távoli hozzáférés esetén kötelező a minimum kétfaktoros azonosítás alkalmazása.

8. Informatikai eszközök üzemeltetésének logikai biztonsága

8.1. Szerverek

1. Az Intézmény informatikai eszközeiről (szerverek, kliensek, perifériák), annak alkotóelemiről és működési beállításairól, a menedzselt felhasználói csoportokról és jogosultsági beállításokról a rendszergazdának dokumentált nyilvántartást kell vezetnie.
2. A szerverek konzoljáról a bejelentkezés csak rendszergazdai jelszó által lehetséges.

3. A szervereken tárolt adatok, a merevlemez fizikai meghibásodása esetén bekövetkező adatvesztés elleni védelmét az alkalmazott RAID technológia biztosítja.
4. A Windows alapú szervereken központi antivírus programrendszer használata kötelező.
5. A szerverek és a központi informatikai alkalmazások működését a központi monitoring rendszeren keresztül a rendszergazdának folyamatosan ellenőriznie kell.

8.2. Személyes adatokat tartalmazó fájl-megosztások és alkalmazások biztonsága

1. A személyes adatokat is tartalmazó fájl-megosztásokhoz, adatbázisokhoz való hozzáférés:
   - csak azoknak a felhasználói csoportoknak adhatók, akik munkakörüknél fogva azokat használják;
   - csak szigorúbb, külön hozzáférési azonosítási eljárás alapján valósítható meg;
   - különleges személyes adatokat is tartalmazó fájlok illetve adatbázisok esetén minden hozzáférésnek a rendszergazda által monitorozhatónak (loggolhatónak) kell lennie.
2. A személyes adatokat is tartalmazó fájl-megosztások, adatbázisok mentésének titkosítva kell történnie.

8.3. Munkaállomások és perifériák

1. A munkaállomások konfigurálását, a felhasználóinak beállítását a rendszergazdának kell végeznie.
2. Bármely munkaállomásra az alapkonfigurációnak tekinthető programokon túl csak a feladatok elvégzéséhez szükséges további programok telepíthetők.
3. A felhasználói munkaeszközök karbantartása a rendszergazda feladata.
4. A munkaállomásokon az operációs rendszer és a telepített alkalmazások biztonsági frissítéseinek használata kötelező.
5. A munkaállomásokon keresztül a hálózatba való bejelentkezés a rendszergazda által a szerveren beállított felhasználók számára biztosított.
6. A munkaállomásokon a jelszavas képernyővédő beállítása és használata kötelező.
7. A Windows alapú munkaállomásokon egységes antivírus programrendszer központi beállítása és használata kötelező. A vírusminták rendszeres frissítésének beállítása, annak kikapcsolási tiltásának beállítása kötelező.
8. A munkaállomásokra csatlakoztatott külső adathordozók (pl. pendrive, mobil HDD, ...) csatlakoztatás utáni azonnali automatikus vírusellenőrzésének beállítása kötelező.

9. A hordozható informatikai eszközön személyes adatokat tartalmazó fájlokat, adatbázisokat titkosított partíción kell tárolni. Ennek feltételeinek biztosítása a felhasználó számára a rendszergazda feladata.

10. A felhasználásból kivont, elavult eszközök biztonságos megsemmisítése a rendszergazda feladata. Az eszközök adathordozójának fizikai megsemmisítése (működésének, adatvisszanyerés lehetőségének megszüntetése) a szintén rendszergazda feladata. A megsemmisítés tényállását a számviteli rendszeren keresztül, selejtezési jegyzőkönyvben kell rögzíteni.

11. Rendszergazda felelőssége, hogy jelentse az intézmény vezetőnek amennyiben bármilyen visszaélést, szabálysértést észlel.

9. Mentési szabályok

1. Az informatikai rendszerekre megfelelő, dokumentáltan szabályozott adatmentési és visszaállítási eljárásokat kell működtetni.

2. A mentések készítésére vonatkozó szabályzásban (nyilvántartásban) – különösen a személyes adatokat tartalmazó adatbázisok, fájl-szerverek mentése esetén – tételesen meg kell adni a következőket:

   - a mentendő berendezéseket,
   - a mentésre kerülő adatok, adatbázisok azonosítását,
   - a mentések módját (pl. teljes, részleges, inkrementális, stb.) és ciklusidejét,
   - a mentések elvégzésének időpontját ill. időtartamát,
   - a mentések automatizált vagy kézzel indított voltát,
   - a mentésért felelős személyt,
   - a mentések titkosítását és annak módját (amennyiben szükséges);
   - a mentések tárolásának módját és helyét,
   - a mentések tárolási idejét (meddig visszaállítható egy adat),
   - a mentések elvégzése naplózásának módját,
   - a mentések nyilvántartásának módját és felelősét,
   - a mentések visszaállítási próbáinak szabályozott időciklusát, és elvégzésének módját, és a visszaállítási próbák dokumentálását.

3. Az üzemeltetés, karbantartás napi hibajavítási feladatainak ellátásához szükséges mentéseket úgy kell elhelyezni, hogy a folytonos üzemvitel megszakadása esetén a helyreállítás a lehető leghamarabb megtörténhessen. A tárolás helyét úgy kell meghatározni, hogy a mentések elérhetősége bármely időszakban (normál munkaidőben vagy azon kívül) biztosított legyen.

4. A tartalék mentések tárolását más, azonos káresemény általi sérüléstől védett helyen kell biztosítani.

5. A mentések – különösen a személyes adatokat tartalmazó adatbázisok, fájl-szerverek mentése esetén – tárolásának szabályait úgy kell kialakítani, hogy a mentésekhez csak az arra jogosult rendszergazdák férhessenek hozzá.

10. Titkosítási szabályok

1. Hordozható informatikai eszközökön (pl. notebook, laptop, ipad, iphone, okos-telefon, stb.) és passzív adathordozókon (pl. pendrive, flashdrive, mobil HDD, stb.) tárolt személyes adatokat is tartalmazó fájlok, adatbázisok csak titkosítottan tárolhatók. Ezen eszközök és adathordozók esetében a titkosítási alkalmazás beállítása a rendszergazda feladata és felelőssége.
2. Külső ügyfélnek küldött levélben érzékeny személyes adatokat tartalmazó fájlok, adatbázisok sima mellékletben nem küldhetők, csak megfelelő erősségű titkosítás alkalmazásával. A levelezés titkosításának, vagy a küldendő állományok titkosításának megfelelő beállítása és a felhasználók számára annak betanítása a rendszergazda feladata és felelőssége.
3. Érzékeny (esetleg különleges) személyes adatok feldolgozó, kezelő adatbázisok használata esetén:
   - a szoftvergyártó által küldött új verziók az Intézmény általi kipróbálására a tesztrendszert és az éles működő rendszert egymástól élesen el kell választani;
   - a tesztrendszeren, és kiemelten a fejlesztők által hiba-meghatározásra használt tesztrendszeren az éles, valós adatbázis, vagy annak akármelyik (régebbi) mentési állapotának feltöltése tilos;
   - tesztelés, valós rendszeren előforduló hibás működés hibájának beazonosítása célú futtatás számára az éles adatbázis egyik mentése használható oly módon, hogy a tesztelésre való feltöltés előtt az adatbázis ***anonimizálás***ra kerül, vagy a tesztelés utáni visszatöltési igény esetén álnevesítésre kerül.

11. Új informatikai rendszerek tervezésére vonatkozó biztonság (privacy by desingn)

Az Intézmény új, személyes adatot kezelő informatikai rendszere bevezetésekor az adatvédelemi felelős bevonásával az intézményvezető feladatai:

1. Az informatikai rendszer általi adatkezelés céljának, jogalapjának és adatkezelési alapelvek megfelelőségének, valamint a kezelt személyes adatok adatbiztonsági hiánya (pl. illetéktelen adathozzáférés, adatvesztés, adatmódosítás vagy adatszivárgás) általi lehetséges károk és kockázatok mértékének vizsgálata.
2. Az informatikai rendszer számára – a vizsgálat alapján feltárt kockázatok mértékének megfelelően – a következők, mint követelmények meghatározása:
   - az informatikai rendszer által támogatott, a jogalapoknak, alapelveknek megfelelő adatkezelési tevékenységek támogatása, mint működési modell;

- a meghatározott adatbiztonsági kockázatokat kezelni tudó adatbiztonsági szintnek megfelelő adatbiztonsági funkciók, működés támogatása;
- a vizsgálatok és a meghatározott követelmények dokumentálása.

3. Csak olyan új informatikai rendszer pályáztatható, terveztethető, vásárolható meg és vezethető be, amely a meghatározott adatbiztonsági követelményeket funkcionalitásában, és működtetése során biztosítani tudja.

12. It üzletmenet-folytonosság és katasztrófa-elhárítás

1. Adatvédelmi szempontból IT üzletmenet-folytonossági tervet illetve IT katasztrófa-elhárítási (pontosabban katasztrófa-állapot utáni visszaállítási) tervet – azaz IT BCP-DRP tervet – akkor kell készíteni, hogyha a személyes adatokat kezelő egy vagy több informatikai rendszer olyan hosszú időre leáll vagy működésképtelenné válik, hogy az Intézmény számára egyik vagy több személyes adatokat kezelő tevékenységének emiatt bekövetkező leállása már az Intézmény vagy az adatkezelésben érintett személyek számára nagyon komoly károkat jelent.
2. Az IT BCP-DRP terv célja az adott személyes adatokat kezelő informatikai rendszerek működésének visszaállítása
   - (az Intézményvezető által) meghatározott rövid időn belül akár a saját eredeti IT erőforráson, akár másik ideiglenes erőforrással, és az adott személyes adatot kezelő tevékenység működésének (teljes vagy részleges) biztosítása;
   - (az Intézményvezető által) meghatározott időn belül a teljes működésnek visszaállítása, beleértve a teljes informatikai rendszer normális működését és az az által támogatott személyes adatkezelési folyamatok teljes működését.
3. A személyes adatokat kezelő informatikai rendszerekre (informatikai rendszerenként külön-külön) el kell készíteni dokumentáltan a következőket:
   - Az informatikai rendszer által támogatott személyes adatkezelési tevékenységek listája, és az azok által megengedett azon maximális leállási idő (RTO), amin belül az az által támogatott személyes adatkezelési tevékenységek közül a legelsőnek mindenképp újra kell tudnia indulni.
   - Az informatikai rendszer által támogatott személyes adatkezelési tevékenységek végzése során a nem tervezett leállás miatti megengedetett legnagyobb adatkiesési időtartama (RPO), amennyi működési idő alatt felvitt adatot a rendszer elveszthet, azaz még utólag jelentősebb veszteség nélkül pótolható.
   - Az informatikai rendszer mentési rendjének szabályozásakor mentési ciklusát úgy kell szabályozni, hogy az a meghatározott RPO értékű vagy annál kisebb lehet. A mentések tárolási helyét úgy kell szabályozni, hogy legalább egy mentés elérhető, a szerver közvetlen működésétől független és kellően biztonságos, védett fizikai környezetben legyen.
   - Meg kell határozni az informatikai rendszer működtetéséhez minimálisan szükséges informatikai infrastruktúrát, beleértve a hardver és szoftver környezetet, illetve a felhasználók számára a hálózati elérési feltételeket is.

- Meg kell határozni azt a tevékenységi forgatókönyvet, amivel – az eredeti működtetési informatikai infrastruktúra működésképtelensége esetén – a helyettesítő minimális informatikai infrastruktúra létrehozható, konfigurálható, azon az adott informatikai rendszer a legutolsó (RPO-nak megfelelő) mentésű adatokkal visszatölthető, és a felhasználók számára újra működőképesen elérhetővé tehető. (A virtuális környezetek kialakítása és használata ebben sokszor segít.) Ezt úgy kell megtervezni, hogy ez az RTO időn belül végrehajtható legyen.

4. Ezt a kialakított forgatókönyvet (ez maga az IT BCP-DRP) működésre legalább induláskor, majd meghatározott ciklikussággal (ajánlott évente minimum egyszer) dokumentáltan letesztelni, kipróbálni kell.

13. Záró rendelkezések

Jelen szabályzat 2020.06.30. napján lép érvénybe. Az érvénybelépéssel egy időben a 2018. 05.25.-től hatályos IT Üzemeltetési Adatvédelmi Szabályzat V_1 érvényét veszti.

Jelen szabályzatba foglaltak a munkavállalók és egyéb közreműködők részére történő megismertetése az adatkezelő Intézményvezető feladata és felelőssége.

Jelen szabályzat felülvizsgálatáért és aktualizálásáért az intézmény vezetője felel.

Budapest, 2020. június 17.

Budapest Főváros XV. kerületi Önkormányzat Újpalotai Összevont Óvoda

Turóczyné Ungvári Edit
óvodavezető