Informatikai Biztonsági Szabályzat

Hatályba lépés dátuma: 2026. július 8.

Készítette, dokumentum változástörténet

Dátum	Szerző	Verzió	Módosítás tárgya
2014.11.06.	Biró Gergely Ganev Attila	1.0	Átadott verzió
2016. 07. 21.	Biró Gergely Ganev Attila	1.1	Törvényi változások alapján felülvizsgált verzió
2017. 03. 08.	Biró Gergely Ganev Attila	1.2	Törvényi változások alapján felülvizsgált verzió
2018.08.08.	Biró Gergely Ganev Attila	1.3	Hivatali informatikai változásai alapján felülvizsgált verzió
2018.10.15.	Biró Gergely Ganev Attila	1.4	NEIH észrevételek alapján felülvizsgált verzió
2021.08.02	Biró Gergely Ganev Attila	1.5	Felülvizsgált verzió
2023.08.29	Biró Gergely Ganev Attila	1.6	NKI észrevételek alapján felülvizsgált verzió
2026.06.29.	Biró Gergely Ganev Attila Fazekas Viktória	1.7	Jogszabályi változások alapján felülvizsgált verzió

Ellenőrizte

Dátum	Név	Verzió	Aláírás

Jóváhagyta

Dátum	Név	Verzió	Aláírás
2026.07.07	Kovács Tibor	1	Kovács Tibor

POLGÁRMESTERI HIVATAL
JÁSZ-NAGYKUN-SZOLNOK VÁRMEGYE
KENDERES

TARTALOMJEGYZÉK

1. INFORMATIKAI BIZTONSÁG

A Kenderes Polgármesteri Hivatal (a továbbiakban: Hivatal) a jogszabályi előírásoknak megfelelően kialakítja és bevezeti az Informatikai Biztonsági Szabályzatát (a továbbiakban: IBSZ, Szabályzat), amely egységes értelmezéssel, meghatározott felelősségi körökkel és eljárásrendekkel támogatja az informatikai rendszerek biztonságának megerősítését és fenntartását.

1.1. AZ IBSZ CÉLJA

A jelen Informatikai Biztonsági Szabályzat meghatározza a biztonsági intézkedéseket a Hivatalnál működtetett informatikai rendszerre vonatkozóan a jogszabályi elvárások alapján.

A Hivatal több elektronikus információs rendszert is használ, amelyeket a kezelt adatok alapján a „a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (továbbiakban: Kibertv.)" és a „7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről" alap biztonsági osztály előírásai szerint kell védeni. A külső szolgáltatótól igénybe vett adatkezelő szolgáltatások esetében a Hivatalnak csak a saját informatikai infrastruktúrájában kell teljesítenie a jogszabályi elvárásokat, de a szolgáltatótól is meg kell követelnie a szükséges védelmet a vonatkozó szerződésben.

Az IBSZ tartalmazza a jogszabályi előírások alapján az adminisztratív, logikai és fizikai védelmi intézkedéseket.

Az IBSZ meghatározza az informatikai szerepköröket, és előírja az egyes érintett személyek informatikai biztonságot érintő feladatait.

A célok elérése érdekében a védelemnek működnie kell az egyes rendszerelemek fennállásának teljes ciklusa alatt – a megtervezéstől az alkalmazáson (üzemeltetésen) keresztül a felszámolásukig.

A Hivatal célja, a jogszabályi előírások szerinti „alap biztonsági osztály" elérése, ezért a törvényi előírásoknak nem megfelelő szabályzatok javítására és a szükséges feladatok elvégzésére Cselekvési tervet készít.

1.1.1. VEZETŐI ELKÖTELEZETTSÉG

Az informatikai rendszer folyamatos és rendeltetésszerű működésének biztosítása az erőforrások és adatok bizalmassági, sértetlenségi, és rendelkezésre állási fenyegetettségének a minimumra csökkentése, a számon kérhetőség és a garanciák biztosítása folyamatos törekvésünk.

A szervezet vezetése kinyilvánítja akaratát, az adatok elvárható bizalmasságára, sértetlenségégének, és rendelkezésre állásának biztosítására. Működésünk során a kockázatokkal arányos módon eleget teszünk a jogszabályi követelményeknek, partnereink és ügyfeleink jogos elvárásainak. A vezető elkötelezettség magába foglalja az elektronikus információs rendszerek teljes életciklusát, amely magába foglalja többek között:

- beszerzés,
- kockázatok elemzése, kezelése,
- biztonsági elemzések készítése, kezelése,
- üzemeltetés,
- biztonsági események kezelése,

- üzletmenetfolytonosság biztosítása,
- selejtezés.

Biztonsági rendszerünk eredményességének fejlesztése érdekében a kockázat értékelések eredményét folyamatosan visszacsatoljuk biztonsági rendszerünk és folyamataink működésébe.

A Hivatal folyamatosan monitorozza saját biztonsági rendszerét és folyamatosan továbbfejleszti.

A szervezet minden dolgozója tudatában van az információ biztonság fontosságának, mindennapi munkájuk során mindent megtesznek az informatikai biztonság fenntartása és fejlesztése érdekében.

1.2. AZ IBSZ HATÁLYA

Az Informatikai Biztonsági Szabályzat (továbbiakban IBSZ vagy szabályzat) személyi hatálya kiterjed a Hivatal

- minden munkatársára,
- azon személyekre, akik a Hivataltól kapott megbízásuknál fogva a Hivatal Informatikai Biztonsági Szabályzatában előírt rendelkezésekkel kapcsolatba kerülnek (szolgáltatók, szerződéses partnerek).

Harmadik személyekkel szemben minden esetben jelen Szabályzat rendelkezéseinek betartásával kell eljárni!

A Hivatal vendég hálózatát használó személyekkel csak az IBSZ 5.8.1.2 Az Internet használatával kapcsolatos szabályok, biztonsági előírások fejezetét kell megismertetni, és csak ezen szabályozások betartása kötelező. A tájékoztatót a vendég hálózathoz való csatlakozáskor kell megjeleníteni és annak elfogadása után engedélyezheti a rendszer az internet használatot.

Az IBSZ tárgyi hatálya kiterjed a Hivatal tulajdonát képező, továbbá a Hivatal által használt épületekben lévő:

- irodák, személyek rendelkezésére bocsátott, vagy általuk tárolt valamennyi informatikai berendezésre, beleértve a berendezések műszaki dokumentációját is,
- rendszerprogramokra és a felhasználói programokra,
- elektronikus adatok teljes körére, keletkezésük és felhasználásuk, valamint feldolgozásuk helyétől, továbbá a megjelenési formájuktól függetlenül,
- adathordozókra, azok tárolására és felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhoz történő eljuttatás folyamatait is,
- az informatikai folyamatban szereplő valamennyi dokumentációra.

Az IBSZ területi hatálya kiterjed a tárgyi hatálya alá tartozó informatikai erőforrások üzemelési helyszíneire:

- a Hivatal épületére

Az IBSZ időbeli hatálya:

- a Szabályzat az aláírás napját követő első munkanapon lép hatályba, a dokumentumba foglalt feladatok és szabályok ezen időponttól alkalmazandók azzal, hogy a hatályba lépéskor folyamatban lévő ügyekre is alkalmazni kell;
- a Szabályzat visszavonásig hatályos.

1.3. A SZABÁLYZAT FELÜLVIZSGÁLATA

Az Informatikai Biztonsági Szabályzat felülvizsgálatát el kell végezni:

- jelentős informatikai, jogszabályi vagy szervezeti változást követően 30 napon belül,
- naplózásiban, üzemeltetésben, fizikai beléptetésben bekövetkezett változások esetén, évente legalább egy alkalommal.

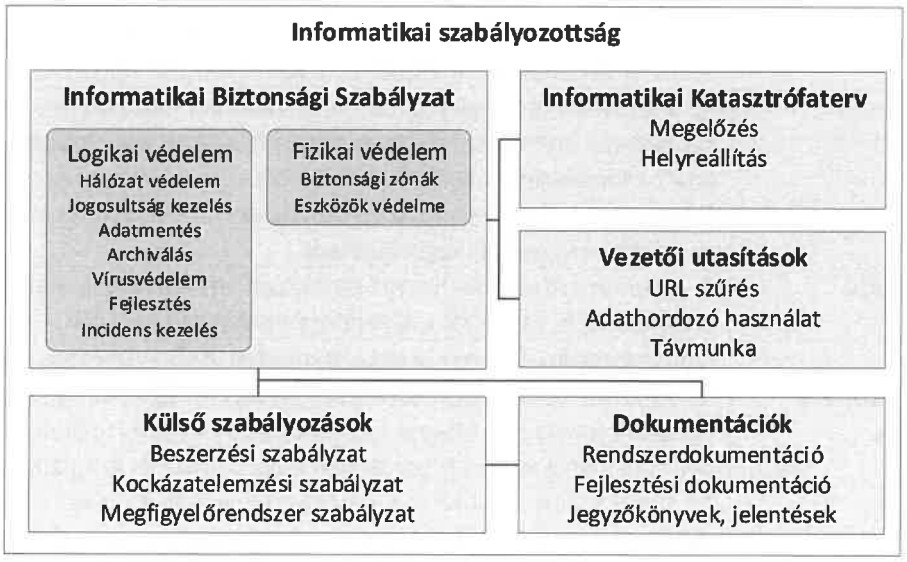
A felülvizsgálat során figyelembe kell venni a jogszabályi változásokat, a technológia fejlettségi szintjét, a hatóság ajánlásokat elvárásokat.

A felülvizsgálatot az informatikai biztonsági felelős kezdeményezi és végzi, az informatikus és jegyző, illetve a jegyző döntésnek megfelelően az általa kijelölt személy (pl: jogász, adatvédelmi tisztviselő, stb.) véleményezi az elkészült dokumentumot.

A szabályzatot a jegyző hagyja jóvá és lépteti hatályba, illetve az általa megbízott személy teszi elérhetővé az arra jogosultak számára, jogosultságaiknak megfelelően.

1.4. A SZABÁLYRENDSZER FELÉPÍTÉSE

A jogszabályi előírások teljesítéséhez szükséges informatikai szabályozások, eljárásrendek, dokumentációk egymáshoz való viszonyát az alábbi ábra szemlélteti.



1.5. FOGALMAK, MEGHATÁROZÁSOK

Az IBSZ-ben használt fogalmak meghatározásai a mindenkor hatályos jogszabályok alapján (kivonat):

Fogalom	Definíció
Adat	Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.
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.
Adathordozó	Adathordozónak nevezzük az informatikai rendszertől elválasztható adattároló eszközöket. (CD, DVD, mobil merevlemez)
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.
Auditálás	Előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés.
Bejelentés-köteles szolgáltatás	Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § j) pontjában meghatározott szolgáltatás.
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.
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

Fogalom	Definíció
	biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.
Biztonsági osztály	Az elektronikus információs rendszer védelmének elvárt erőssége.
Biztonsági osztályba sorolás	Kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása.
Dokumentum	Számítástechnikai eszközökkel készített irat (fájl), ilyen lehet például Word szövegszerkesztővel vagy Excel táblázatkezelővel készített állomány, stb.
EGT-állam	Az információs önrendelkezési jogról és az információszabadságról szóló törvényben meghatározott állam.
Elektronikus információs rendszer	a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat, b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.
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.
Esemény	Az esemény a felhasználó által érzékelt váratlan jelenség, amely károsan hat az informatikai biztonságra, ezen keresztül az informatikai szolgáltatásokra.
Életciklus	Az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam.
Éles környezet	Számítógépes rendszerek azon részei, ahol a tényleges szolgáltatásokat nyújtó szoftverek üzemelnek.
Észlelés	A biztonsági esemény bekövetkezésének felismerése.
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 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.
Hitelesség	Egy információ hiteles, ha minden kétséget kizáróan megállapítható annak előállítója és az a tény, hogy az előállítás óta változatlan maradt.
Hozzáférés	Olyan eljárás, amely lehetővé teszi valamely informatikai rendszer használója számára, hogy a rendszerben lévő adatokat elérje (írás, olvasás, módosítás, törlés, stb.).

Fogalom	Definíció
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.
Informatikai katasztrófa	Egy olyan nem kívánt esemény, amely az adattovábbító, -tároló és -feldolgozó képesség elvesztését okozza hosszabb időre, vagy fizikailag megsemmisül.
Informatikai Katasztrófaterv	Olyan dokumentum, amely tartalmazza azon eljárásokat, amelyekkel az informatikai rendszer kritikus információ feldolgozó képességei helyreállíthatók elfogadhatóan rövid idő alatt a szükséges aktuális adatokkal katasztrófa után.
Informatikai katasztrófahelyzet	Az az állapot, amikor az informatikai rendszer utolsó működőképes állapotát az üzemeltetési szabályok előírásszerű betartásával és végrehajtásával, a meghatározott erőforrások felhasználásával a megállapított helyreállítási időn belül nem lehet visszaállítani.
Internet	Világméretű számítógép-hálózat, amely a különböző rendszerű számítógép-hálózatok ezrei között egy egységes „hálózati társalgási nyelv" – az Internet Protocol – segítségével kommunikációt tesz lehetővé.
Katasztrófa elhárítás tervezés	Lehetővé teszi, hogy egy esetleges katasztrófa bekövetkezte után az informatikai szolgáltatásokat ellenőrzött módon, egy előre megállapított szinten helyreállítják, oly módon, hogy előre meghatározzák a helyreállítás során érvényes személyi felelősségeket, illetve a követendő tevékenységeket.
Kockázat	A fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.
Kockázatelemzés	Az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.
Kockázatkezelés	Az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása.
Kockázatokkal arányos védelem	Az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.
Kritikus adat	A személyes adat vagy valamely jogszabállyal védett adat.
Logikai védelem	Az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.
Megelőzés	A fenyegetés hatása bekövetkezésének elkerülése.
Mobil eszköz	Minden olyan informatikai eszköz, mely adat továbbításra, feldolgozásra, tárolásra alkalmas. (okostelefon, laptop, tablet)
Reagálás	A bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés.
Rendelkezésre állás	Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
Rendszermonitorozó eszközök	Az informatikai rendszerről gyűjtenek működési és biztonsági információt és valamilyen csoportosító szempont alapján megjelenítik ezeket.

Fogalom	Definíció
Rendszerprogram	Olyan alapszoftver, de nem operációs rendszer, mely biztosítja, az informatikai rendszer hardvereinek használatát és az alkalmazói programokat működését, futtatási környezetét.
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.
Súlyos biztonsági esemény	Olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.
Szervezet	Az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető.
Teljes körű védelem	Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.
Teszt-környezet	Olyan hardver és szoftverkörnyezet, melyen az éles kiadás terítése előtti program, illetve rendszer-tesztelések zajlanak az éles környezethez hasonló körülmények között.
Tűzfal (firewall)	A tűzfal akadályt jelent a helyi és a külső hálózat között, melyen bizonyos forgalom egyik vagy mindkét irányban nem mehet keresztül, ill. valamilyen további ellenőrzésen megy keresztül. A tűzfalak rendszerint folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek, felhasználók azonosítóit, rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak.
Védelmi feladatok	Megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés.
Virtualizáció	A virtualizáció egy keret rendszer vagy módszer, a számítógép erőforrásainak felosztására, egy többszörös megvalósító környezetre, alkalmazva egy vagy több koncepciót vagy technológiát.
Visszatöltés	Ezzel a funkcióval a korábban a "Mentés" funkcióval lementett adatokat állíthatók helyre. Ilyenkor visszaáll az adatbázis mentéskori állapota, az azóta bevitt adatok, módosítások elvesznek!

1.6. AZ INFORMATIKAI BIZTONSÁGGAL KAPCSOLATOS SZEREPKÖRÖK

Az IBSZ-ben a Hivatal szervezeti felépítésével összhangban a következő főbb felelősségi körök jelennek meg.

1.6.1. FELHASZNÁLÓ

Egy adott elektronikus információs rendszert igénybe vevők köre. A felhasználó az informatikai rendszerekhez hozzáféréssel rendelkező munkatárs, aki alkalmazza az IBSZ-ben és egyéb kapcsolódó szabályzatokban meghatározott biztonsági intézkedéseket. Feladatai:

a) felettes vezető vagy az adatgazda felé jelzi a jogosultság igényt

b) a Hivatal informatikai rendszereit kizárólag azok céljaival megegyezően használni,

c) a Hivatal informatikai rendszerén csak a számára engedélyezett erőforrásokat használni,

d) a munkával kapcsolatos dokumentumok közös meghajtón tárolása,

e) tudomására jutott, feltételezett biztonsági incidensek jelzése az informatikus felé,

f) meghibásodás, üzemzavar észlelésekor, vírusfertőzés (vagy annak gyanúja) esetén haladéktalanul értesíteni az informatikust, a számítógép további használatát az informatikus intézkedéséig felfüggeszteni,

g) a munkavégzésre adott eszközök rendeltetésszerű használata, leltározáskor és más ellenőrzéskor történő bemutatása, a jogviszony/munkaviszony megszűnésekor az eszközök visszaszolgáltatása,

h) a hálózati szolgáltatások igénybevételéhez használatos jelszavait titkosan történő kezelése, a jelen Szabályzat jelszóhasználattal kapcsolatos előírásainak betartása,

i) „Tiszta asztal, tiszta képernyő" politika betartása,

j) az IBSZ-t megismerni, az abban foglaltakat betartani, valamint együttműködni a Hivatal informatikai rendszereinek üzemeltetőivel a hatékony munkavégzés és a megfelelő IT biztonsági szint fenntartása érdekében,

k) a számára biztosított informatikai eszközöket, berendezéseket nem bonthatja meg, a hardver és szoftverkörnyezetet - beleértve a számítógépes vírusellenőrzéssel, és vírusirtással kapcsolatos szoftvereket is - nem módosíthatja, az eszközök hálózati és egyéb beállításaiban működést befolyásoló módosításokat nem végezhet,

l) felelősséget vállalni az általa szándékosságból, gondatlanságból, vagy a neki felróható módon az általa, a nevében, a felhasználói azonosítójával (különösen: a jelszavak kölcsönadásával vagy nem biztonságos kezelésével, a hozzáférési jogosultságok nem megfelelő kezelésével, a számára biztosított - Hivatal tulajdonát képező - informatikai, kommunikációs eszközökben vagy eszközökkel) okozott szabályellenes cselekedetekért, károkért

m) az informatikus kérésére hibaelhárítás vagy hibamegelőzés folyamán vele együttműködni, számára a szükséges információkat megadni,

n) USB eszközök, vagy más külső adathordozók csatlakoztatása után meggyőződni, hogy a számítógépes vírusellenőrző eszköz a vírus ellenőrzést, vírusirtást végrehajtotta, ezért a használni kívánt eszköz vírusmentes, a tevékenységhez (szükség esetén) az informatikus segítséget nyújt,

o) amennyiben tudomására jut, hogy bárki megsértette a jelen Szabályzatban foglaltakat, haladéktalanul tájékoztatni az informatikai biztonsági felelőst és az informatikust, akik az IT biztonsági incidenst rögzítik.

1.6.2. FELETTES VEZETŐ (ALJEGYZŐ)

Felelős, hogy minden a hozzárendelt munkatárs rendelkezzen a feladatainak ellátásához szükséges jogosultsággal, ismerettel. Az 1.6.1 Felhasználó fejezetben megfogalmazott elvárásokon felül az alábbi feladatok elvégzéséért felelős:

a) jogosultság igénylések indítása saját hatáskörben vagy felhasználói igény alapján,

b) email címek, postafiókok igénylése,

c) betartatja az informatikai biztonsági szabályzat előírásait

d) jelzi a munkatársak oktatási, képzési igényét,

e) jelzi hozzárendelt munkatársak munkavégzéséhez szükséges hardver, szoftver igényt,

f) engedélyezi az eszközök eseti kivitelét a Hivatal területéről,

g) munkafolyamatok kritikusságának meghatározása, jóváhagyása.

1.6.3. ADATGAZDA

A Hivatal informatikai rendszerének adatgazdája az a felhasználó, aki az adott rendszerhez jogosultságot állíthat be, vagy külső szolgáltatás esetén jogosultságot igényelhet. Az informatikai rendszerek adatgazdáit a ***Besorolási ív*** tartalmazza.

Az alábbi feladatok elvégzéséért felelős:

a) engedélyezi és beállíttatja a felhasználók munkavégzéséhez szükséges jogosultságokat;

b) ellenőrzi a jogosultságok beállítását, nyilvántartását;

c) betartatja az informatikai biztonsági szabályzat előírásait;

d) meghatározza az adatkezelő folyamatok kritikusságát és helyreállítási idejét, archiválási frekvenciáját.

1.6.4. JEGYZŐ

A Hivatal vezetője, biztosítja a Hivatal informatikai biztonsági rendszer működtetéséhez szükséges erőforrásokat, jóváhagyja a szabályozásokat és intézkedéseket, engedélyezi és felügyeli az informatikai rendszer változásait. Az 1.6.3 Adatgazda fejezetben megfogalmazott elvárásokon felül az alábbi pontokért felelős.

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését;

b) az elektronikus információs rendszer biztonságáért felelős személy kinevezése / megbízása;

c) kijelöli az adatgazdát és az informatikus személyét;

d) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot;

e) kiadja az adatvédelmet és adatbiztonságot érintő jegyzői utasításokat (többek között URL szűrés, adathordozó használat, távoli hozzáférés, stb.);

f) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések és auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak;

g) belefoglaltatja az informatikai és informatikai biztonsági követelményeket az informatikai szolgálatói szerződésekbe;

h) szükség szerint szankcionálja az informatikai biztonsági mulasztásokat;

i) engedélyezi az informatikai biztonsági követelményektől való eltérést;

j) engedélyezi a betekintést a munkavállalók postafiókjába, és/vagy a munkavállalók Hivataltól kapott eszközein tárolt adatokba;

k) biztosítja - a kockázatokkal arányos módon - az elektronikus információs rendszerek biztonságát.

l) biztosítja a fizikai védelem kialakítását;

m) meghatározza a nyilvánosan publikálható adatok körét;

n) engedélyezi a rendszergazdai szintű jogosultságokat;

o) elrendelheti a jogosultságok azonnali visszavonását;

p) engedélyezi a vagyontárgyak selejtezését, értékesítését;

q) ellenőrzi a külső informatikai beszállítóktól megkövetelt informatikai biztonsági feltételek teljesülését;

r) engedélyezi a külső informatikai beszállítók részére a helyszíni- vagy távoli karbantartást;

s) irányítja, meghatározza és ellenőrzi a Hivatal informatikai rendszerének üzemeltetését;

t) biztosítja az információvédelmi feladatok folyamatos belső ismertetését, a képzési terv kidolgozását és oktatását;

u) engedélyezi az eszközök eseti kivitelét a Hivatal területéről;

v) engedélyezi az informatikai rendszer védelmét, elérését, alapvető működését, érintő változásokat;

w) elrendeli és ellenőrzi az informatikai rendszerrel kapcsolatos üzemeltetői tesztek (adatmentés teszt, katasztrófaterv teszt) végrehajtását, gondoskodik a tesztek kiértékeléséről;

x) engedélyezi az adatmentések, archiválások helyreállítását;

y) évente legalább egy alkalommal felülvizsgáltatja az üzemeltetési feladatokat tartalmazó előírásokat.

1.6.5. INFORMATIKUS

Az informatikus kiemelt jogosultságokkal rendelkező felhasználó, aki működteti az informatikai rendszereket és alkalmazza az előírt biztonsági intézkedéseket, javaslatokat tesz változtatásokra, amivel az információbiztonság hatékonysága javítható. Feladata többek között:

a) informatikai eszközök beüzemelése, üzemeltetése, karbantartása, felügyelete,
b) alkalmazza az előírt biztonsági intézkedéseket,
c) végrehajtja a jegyző által meghatározott üzemeltetési és ellenőrzési feladatokat;
d) naprakészen vezeti a hardver-szoftver nyilvántartásokat dokumentálja a változásokat,
e) meghatározza, dokumentálja a Hivatal által használt informatikai rendszerek alapkonfigurációját,
f) vezeti és folyamatosan naprakész állapotban tartja az üzemeltetéshez kapcsolódó dokumentációkat,
g) jogosultsági csoportok kialakítása,
h) elkészíti a Hivatal informatikai költségvetési tervét;
i) jogosultság igénylő lapok őrzése, nyilvántartás naprakészen tartása
j) jogosultságok kezelése, (beállítása, módosítása, letiltása, törlése)
k) informatikai katasztrófaterv és adatmentés helyreállítási tesztek elvégzése,
l) részvétel az üzletmenet-folytonosságiterv tesztelésben,
m) informatikai rendszer karbantartásának tervezése,
n) informatikai adatfeldolgozói szolgálatásokat nyújtó szolgáltatókkal kapcsolat tartás,
o) üzemeltetési és biztonsági naplók vizsgálata,
p) informatikával kapcsolatos karbantartási feladatot végző külsősök felügyelete,
q) felhasználók részére eszközök kiadása, visszavonása,
r) informatikai dokumentációk elkészítése, változások dokumentálása,
s) javaslattétel informatikai fejlesztésekkel kapcsolatban, költségvetési terv készítése,
t) a Hivataltól kapott eszközökön tárolt fájlokhoz, postafiókokhoz hozzáférés biztosítása, jegyző által meghatározott személy részére,
u) tűzfaleszközök konfigurálása,
v) vírusvédelmi rendszer kialakítása, üzemeltetése, dokumentálása,
w) biztonsági mentés, archiválás tervezése, kialakítása, dokumentálása,
x) biztonsági mentések állapotának napi szintű dokumentált ellenőrzése,
y) URL szűrés beállítása, adathordozók használatának technikai szabályozás a jegyzői utasítás szerint,
z) informatikai biztonsági incidensek kivizsgálása.

1.6.6. INFORMATIKAI BIZTONSÁGI FELELŐS

Feladata a Hivatal informatikai biztonságának folyamatos fenntartása és fejlesztése, a biztonsági kockázatok minimalizálása, valamint a munkavállalók biztonságtudatosságának növelése.

Az informatikai biztonsági felelős feladatai és felelősségei közé tartozik:

a) gondoskodik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) gondoskodik a kockázatkezelési keretrendszer szerinti tevékenységek tervezéséről, szervezéséről, koordinálásáról, elvégzéséről és ellenőrzéséről,

c) előkészíti és a Hivatal vezetőjének jóváhagyását követően megküldi a nemzeti kiberbiztonsági hatóság részére a Hivatal információbiztonsági szabályzatát,

d) előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását,

e) előkészíti és az jegyző egyetértésével kezdeményezi a nemzeti kiberbiztonsági hatóságnál a Hivatal elektronikus információs rendszereivel kapcsolatos engedélyezési eljárásokat,

f) megtartja vagy megszervezi a továbbképzésre kötelezett személyek részére jogszabályban előírt továbbképzéseket,

g) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal elektronikus információbiztonságot érintő szabályzatait és szerződéseit,

h) folyamatos és tervezett ellenőrzéseket végez annak vizsgálatára, hogy a Hivatal elektronikus információbiztonságra vonatkozó belső normáiban lévő előírások hogyan valósulnak meg, ennek megállapításait írásban rögzíti a Hivatal vezetője számára,

i) felülvizsgálja, hogy a Hivatal elektronikus információbiztonságot érintő belső szabályzatai összhangban vannak-e a hatályos jogszabályokkal és a Hivatal belső szabályozóival,

j) az ellenőrzések és az esetleges incidensek tapasztalatai felhasználásával – a fejlesztendő területekre vonatkozó javaslatokat tartalmazó – biztonsági helyzetértékelést készít a Hivatal vezetője számára,

k) legalább évente megvizsgálja az intézkedési tervet és beszámolót készít a Hivatal vezetője számára az előrehaladásról, amiben kiemeli az esetleges lemaradásokat és a rövid távon szükséges intézkedéseket,

l) kapcsolatot tart a nemzeti kiberbiztonsági hatósággal és a kiberbiztonsági incidenskezelő központtal,

m) a Hivatal bármely elektronikus információs rendszerét érintő incidensről tájékoztatja a felettes hatóságot,

n) tájékoztatja a jegyzőt és az informatikust a lehetséges informatikai biztonsági kockázatokról és szakmai segítséget nyújt a megelőzésben, a bekövetkezett incidensek kezelésében.

Az informatikai biztonsági felelős feladatait kiszervezett tevékenység keretében, megbízott szolgáltató látja el. A szolgáltató közvetlenül a jegyzőnek felel, de kapcsolatot tart fenn az informatikussal.

Az informatikai biztonsági felelős feladatainak ellátása során:

- tanácsadással segíti az elektronikus információs rendszerek jogszabálynak megfelelő, biztonságos beállítását, üzemeltetését,
- tanácsadással segíti a cselekvési tervben meghatározott feladatok végrehajtását,
- ellenőrzésekkel megbizonyosodik az elektronikus információs rendszerek jogszabálynak megfelelő működéséről,
- véleményezi az elektronikus információs rendszerekhez kapcsolódó szabályzatok, dokumentációkat, nyilvántartásokat, szerződéseket, dokumentumokat,
- véleményezi a beszerzéseket.

1.6.7. FELELŐSSÉGI KÖRÖK ÖSSZEFÉRHETETLENSÉGEI

Az informatikus és az informatikai biztonsági felelős szerepköröket különböző személyek tölthetik be. Az Informatikai biztonsági felelős független, szervezetileg nem tartozik a Hivatal által irányított szervezeti egységek egyikéhez sem.

A felhasználói, az üzemeltetői, rendszertámogatói és fejlesztői jogosultságokat el kell határolni. Egyazon személy nem lehet felelős a rendszer beállításáért, ellenőrzéséért, változások engedélyezéséért, ezért az alábbi szabályokat be kell tartani:

- szigorúan meg kell osztani a feladatokat és a felelősségeket
- el kell különíteni egymástól a biztonsági ellenőrzést végző személyek feladatait az ellenőrzöttek körétől;
- szoftver fejlesztői jogosultsággal rendelkező személyek nem üzemeltethetik, és nem végezhetnek adatfeldolgozást az általuk fejlesztett rendszerben.

1.7. BESZÁLLÍTÓK

A Hivatal egyes, informatikai rendszerei, adatai – szerződéses kötelezettségekből eredően – harmadik fél számára (szerződéses partner) is hozzáférhetőek lehetnek.

A Hivatal beszállítókkal szembeni kötelezettségeit a 1.7.1 Biztonsági intézkedések harmadik féllel való együttműködés során fejezet tartalmazza.

A beszállítókkal szemben támasztott követelményeket a beszállítókkal kötött szerződésekben kell megfogalmazni az ***Informatikai Beszerzési Eljárásrendnek*** megfelelően.

Az adatok tárolási helyéről a szolgáltatónak a szolgáltatási szerződés megkötése előtt és a szolgáltatási szerződésben is nyilatkoznia kell.

Külön ki kell értékelni biztonsági szempontból, hogy a külső fejlesztő vagy szállító mennyiben rendelkezik lehetőségekkel a rendszer későbbi veszélyeztetéséhez.

Minden olyan esetben, amikor harmadik fél kapcsolódhat be a Hivatal informatikai rendszerébe, az informatikusnak és az informatikai biztonsági felelősnek közösen kockázatbecslést kell elvégeznie, hogy a szükségessé váló különleges óvintézkedéseket meghatározzák.

1.7.1. BIZTONSÁGI INTÉZKEDÉSEK HARMADIK FÉLLEL VALÓ EGYÜTTMŰKÖDÉS SORÁN

Különös gondossággal kell eljárni olyan harmadik féllel szemben, amelynek személyzete nem tartózkodik állandóan a Hivatal irodájában, de időszakos fizikai és logikai hozzáférést kap az informatikai rendszerhez. Ilyenek lehetnek a hardver és szoftver támogatók, karbantartók stb.

A külső informatikai kapcsolatok általános biztonsági követelményei az alábbiak:

- Minden beszállító köteles, a munkájához használt számítógépeken naprakész operációs rendszert és aktív vírusirtó alkalmazást használni.
- A hozzáférési jogosultságok igénylésének, létrehozásának, megszűntetésének, nyilvántartásának előírásai megegyeznek a Hivatal munkatársai esetében alkalmazott szabályokkal, így a 6.1.1 Felhasználói jogosultságok létrehozása és 6.1.2 Felhasználói jogosultságok megszüntetése, megváltoztatása fejezetekben megfogalmazott szabályok szerint kell eljárni.

- Ha külső partner távolról éri el a Hivatal hálózatát, illetve valamely informatikai rendszerét, akkor a biztonságos elektronikus adatcsere kapcsolat érdekében a külső partner köteles a Hivatal által előírt biztonsági megoldásokat (pl.: VPN kapcsolatot) megvalósítani mindazon saját eszközein, amelyekről a távoli elérés lehetséges.
- A Hivatal informatikai eszközeinek beszállítók általi elérése csak biztonságos SSL védett csatornán lehetséges, amelyhez csak megbízható tanúsítvány használható.

A távoli elérést minden esetben naplózni kell, a naplónak az alábbiakat kell minimálisan tartalmaznia:

- kapcsolódás ideje,
- forrás IP cím,
- bejelentkezéshez használt felhasználónév,
- kapcsolat bontásának ideje.

Minden olyan esetben, amikor a Hivatal külső informatikai szolgáltatást vesz igénybe, köteles rendszeresen ellenőrizni, a szolgáltatás során az elvárható és a szerződésben szereplő védelmi intézkedések teljesülését.

Naprakész nyilvántartást kell vezetni, a harmadik fél által elérhető rendszerekről, modulokról. A nyilvántartásnak tartalmaznia kell a beszállító részére létrehozott hozzáférési adatait, jogosultságát. A szerződés lejárta után a hozzáférést meg kell szüntetni a 6.1.2 Felhasználói jogosultságok megszüntetése, megváltoztatása fejezetben leírtaknak megfelelően. A nyilvántartást rendszeresen, évente legalább egy alkalommal felül kell vizsgálni. A harmadik fél részére biztosított hozzáférések szükségességéről, fenntartásáról az érintett harmadik félnek évente nyilatkoznia kell. A harmadik féllel kötött szerződés önmagában nem elégséges a hozzáférések fenntartásához!

2. VAGYONTÁRGYAK KEZELÉSE

Az informatikai rendszerekkel kapcsolatos vagyontárgynak tekintjük:

- információ-vagyontárgyak: adatbázisok és adatállományok, rendszerdokumentáció, használói/kezelői kézikönyvek, oktatási anyagok, üzemviteli, üzemeltetési és támogató eljárások, archivált adatok, biztonsági másolatok;
- szoftver-vagyontárgyak: irodai szoftverek, adatkezelő alkalmazások, szoftver licencek, operációs rendszer, adatbáziskezelő szoftverek, ügyviteli szoftverek, informatikai védelmi szoftverek, stb;
- fizikai vagyontárgyak: számítógépek, szerverek, monitorok, laptopok, modemek, hálózati eszközök (router, switch, stb.), számítógép perifériák, hálózati adattároló eszközök (NAS, Storage, stb.), adathordozók, stb.;
- szolgáltatások: internet kapcsolat, telefonvonal, adatfeldolgozók, interneten keresztül elérhető szolgálatások (email szolgáltatás, VoIP, üzenetküldő szolgálatások, stb.).

A Hivatalnál csak gyártói támogatással rendelkező hardver és szoftver eszközöket lehet használni. A gyártói támogatással nem rendelkező eszközök cseréjéről folyamatosan gondoskodni kell.

2.1. HARDVER- ÉS SZOFTVERESZKÖZÖK NYILVÁNTARTÁSA, KEZELÉSE

2.1.1. A NYILVÁNTARTÁS TARTALMÁNAK MEGHATÁROZÁSA

Minden a Hivatal tulajdonába kerülő hardverről, illetve szoftverről az informatikusnak naprakész nyilvántartást kell vezetnie. A nyilvántartásnak tartalmaznia kell azon szoftver licenceket, amelyekre a Hivatal használati joggal rendelkezik.

A hardver eszközöket (hálózati eszközök, szerver eszközök, UPS, nyomtatók, kliens eszközök) használatba vétel előtt el kell látni azonosító címkével (leltári számmal) és a nyilvántartásba fel kell jegyezni legalább:

- eszköz gyártója, típusa, sorozatszáma, főbb paraméterei,
- eszköz leltári száma,
- beszerzés ideje,
- garancia lejárata,
- eszköz állapota (raktárban, selejt, felhasználónak kiadva),
- telepített szoftverek,
- felhasználóknak kiadott eszközök esetén a felhasználó nevét.

A szoftverekről az alábbi adatokat kell nyilvántartani:

- szoftver gyártója, típusa,
- szoftver sorozat száma,
- beszerzés dátuma,
- licenc mennyisége,

- felhasznált licencek hozzárendelése a hardverhez,
- felhasználóknak kiadott eszközök esetén a felhasználó nevét.

A Hivatal által használt valamennyi szerver és kliens számítógépen meghatározott időközönként, de legalább évente ellenőrizni kell a telepített szoftverek jogtisztaságát, és licensz szerződés szerinti mennyiségét, valamint az eszközök hardver változásait.

A hardver- és szoftvernyilvántartást meghatározott időközönként, de évente legalább egyszer dokumentáltan felül kell vizsgálnia az informatikusnak.

Az audit során ellenőrizni kell:

- a használatban lévő szoftverek rendelkeznek-e licence-el,
- a megvásárolt licencek számának a használt szoftverek mennyiségével arányban kell lenniük,
- a használt szoftverek verziószámát,
- a ténylegesen használt szoftverek megegyeznek-e a szoftverleltárban foglaltakkal.

A vizsgálat lebonyolítása az informatikus feladata, a vizsgálat eredményéről az informatikai biztonsági felelőst és a jegyzőt is tájékoztatni kell.

A felhasználók rendelkezésére bocsátott hardver és szoftver eszközök a Hivatal tulajdonát képezik, amelyek ellenőrzését a jegyző bejelentés nélkül bármikor elrendelheti.

2.1.2. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI OSZTÁLYOZÁSA ÉS KEZELÉSE

Hivatal elektronikus információs rendszereit biztonsági osztályokba kell sorolni a ***Biztonsági Osztályba Sorolási eljárásrend (1. számú melléklet)*** rendelkezései szerint, és a használat vagy kezelés során az osztályba sorolás szerinti védelmi követelményeket kell alkalmazni. A ***Besorolási ív (4. számú melléklet)*** felülvizsgálata az informatikai biztonsági felelős feladata. A ***Besorolási ív (4. számú melléklet)*** felül kell vizsgálni:

- jogszabályi változást követően,
- az elektronikus információs rendszert érintő technikai változás esetén (pl: futtató környezet),
- az elektronikus információs rendszert érintő gyártóval kapcsolatos változás esetén (pl: kontakt infók, szerződés változás).
- elektronikus információs rendszer be vagy kivezetésekor.

Azokat az eszközöket, amelyek (biztonsági szempontból) osztályozott adatot, szoftvert, alkalmazást tárolnak, az osztályozással megegyező módon kell kezelni.

Az osztályozott eszközöket más helyiségbe áthelyezni, vagy a Hivatal területéről kivinni csak a jegyző engedélyével lehet.

Az osztályozott eszközöket az ***Selejtezési Szabályzat (2. számú melléklet)*** szerint kell selejtezni.

2.2. HARDVER- ÉS SZOFTVER ESZKÖZÖK BESZERZÉSÉNEK SZABÁLYAI

Beszerzés esetén a Hivatal az Informatikai Beszerzési Eljárásrend alapján folytatja le a beszerzést.

Az informatikus felelőssége az éves beszerzési tervek összeállítása. Az éves beszerzési terveknek tartalmaznia kell az egyszeri beruházások és a rendszeres, megújuló költségek nevét, darabszámát, várható összegét, a beszerzés várható dátumát. A beszerzési tervekben fel kell tüntetni a gyártói támogatás megszűnése miatt cserélendő eszközöket is.

A beszerzés tervezéskor külön meg kell jeleníteni az informatikai biztonság fenntartására, fejlesztésére vonatkozó beszerzendő tételeket. Az informatikai biztonsági költségek tervezésénél figyelembe kell venni az informatikai biztonsági felelős véleményét.

2.3. HARDVER- ÉS SZOFTVER ESZKÖZÖK SELEJTEZÉSE ÉS ÚJRAFELHASZNÁLÁSA

A selejtezésre vonatkozó előírásokat az ***Informatikai Selejtezési szabályzat (2. számú melléklet)*** tartalmazza.

3. EMBERI ERŐFORRÁSOK BIZTONSÁGA

A humánbiztonság-kezelés az emberi tényezőkkel kapcsolatos kockázatok megelőzésére, kiszűrésére, csökkentésére irányul, amelyhez elsősorban nem adminisztratív eszközöket (a szabályok merev alkalmazását) kell alkalmazni, hanem a humánerőforrás-kezelő folyamatokba kell beépíteni a biztonsági követelményeket is figyelembe vevő egységesített eljárásokat; vagyis a humán menedzsment folyamatokat ki kell egészíteni a biztonsági szempontokkal és követelményekkel.

A humánbiztonság-kezeléssel kapcsolatban az alábbi alapvető (stratégiai szintű) követelmények fogalmazhatók meg::

- Teljes körű védelem: a védelem terjedjen ki minden, adatot előállító, felhasználó és kezelő, személyre, illetve azokra a személyekre, akik az ilyen adatot tároló, feldolgozó és továbbító információs rendszerrel kapcsolatban állnak.
- Zárt védelem: a humánbiztonsági eljárások során ki kell szűrni minden olyan személyt, akinek alkalmazása veszélyeztetheti az információs rendszer biztonságát, és a Hivatal jogi környezete tegye lehetővé az ilyen személyek eltávolítását is.
- Szabályozott védelem: például a hozzáférési és kezelői jogokat az "ismerete szükséges" (need-to-know) elv alapján kell kiosztani.
- Folytonos védelem: a védelem terjedjen ki az emberi erőforrás-fejlesztés teljes életciklusára.
- Kockázatokkal arányos védelem: a személyügyi védelmi ráfordítások (pl. a kompetencia-vizsgálat mélysége) arányosak legyenek a biztonsági kockázatokkal.

3.1. INFORMATIKAI BIZTONSÁGI KÖVETELMÉNYEK A MUNKASZERZŐDÉSBEN

A munkaszerződésekben rögzíteni kell munkatársak felelősségének körét, a jogviszony fennállása utáni kötelezettségeket és ezek megsértése esetén a fegyelmi és felelősségre vonási eljárásokat.

A munkatársat a munkaszerződés megkötésekor tájékoztatni kell a kötelezettségeiről, felelősségeiről, és a felelősségre vonás szabályairól. A munkatársnak ki kell töltenie és alá kell írnia az ***5. sz. melléklet - Alkalmazotti nyilatkozat*** dokumentumot. Az alkalmazotti nyilatkozatokat a jegyző által megbízott személy köteles tárolni.

A munkatárs felettes vezetője felel azért, hogy a munkatársak megismerhessék a rájuk vonatkozó biztonsági szabályokat. Az új belépők tájékoztatása az informatikus feladata.

3.1.1. MUNKAKÖRÖK, SZEREPKÖRÖK BIZTONSÁGA

Minden informatikai eszköz használatát igénylő munkakör, vagy szerepkör esetén meg kell határozni a biztonsági kockázat szempontú besorolását. A munkakörök, szerepkörök biztonsági szempontú besorolását a jegyző által megbízott személy végzi el. A munkakörök vagy szerepkörök biztonsági besorolását és az adott munkakörnél lefolytatandó ellenőrzéseket az alábbi táblázat tartalmazza:

Munkakör, szerepkör kockázati szintje	Munkakör, szerepkör meghatározása	Ellenőrzési követelmények
Alacsony	felhasználók	szakmai, informatikai végzettség ellenőrzése bizonyítványok bekérésével

Munkakör, szerepkör kockázati szintje	Munkakör, szerepkör meghatározása	Ellenőrzési követelmények
Közepes	szervezeti egység vezetők, adatgazdák, felettes vezető	szakmai, informatikai végzettség ellenőrzése kompetencia vizsgálattal, korábbi munkahelyekről történő távozás vizsgálata, erkölcsi bizonyítvány
Magas	informatikus, jegyző	szakmai, informatikai végzettség ellenőrzése kompetencia vizsgálattal referenciák korábbi munkahelyről, korábbi munkahelyekről történő távozás vizsgálata, erkölcsi bizonyítvány

Az ellenőrzéseket új munkatárs felvételekor le kell folytatni. A munkatárs új munkakörbe kerülésekor csak a következőket kell vizsgálni:

- szakmai felkészültség (kompetencia vizsgálat)
- tapasztalatok a munkatárssal kapcsolatban (interjúk felettes vezetővel, közvetlen munkatársakkal)

A munkakörök, szerepkörök biztonsági szempontú besorolását a jegyző hagyja jóvá.

3.1.2. KOCKÁZATOK, KOCKÁZATI BESOROLÁS

Adatvédelmi kockázat

Az adatvédelmi kockázatok meghatározásánál az alábbiak szerint vizsgálni kell, hogy a munkatárs milyen minőségű és milyen mennyiségű adathoz fér hozzá:

- alacsony adatvédelmi kockázat: a munkatárs csak a munkavégzése során kezelt adatokhoz fér hozzá.
- közepes adatvédelmi kockázat: a munkatárs több munkatárs, vagy több szervezeti egység által kezelt adathoz fér hozzá.
- magas adatvédelmi kockázat: minden rögzített információhoz hozzáfér, vagy hozzáférést tud beállítani.

EIR üzemeltetési kockázat

Az EIR üzemeltetési kockázat meghatározásánál az alábbiak szerint vizsgálni kell, hogy a munkatárs milyen jogosultsággal rendelkezik az EIR-ben:

- Nincs üzemeltetési kockázat: a munkatásnak nincsenek adminisztrátor szintű jogosultságai.
- Közepes üzemeltetési kockázat: a munkatás rendelkezik adminisztrátor szintű jogosultsággal a munkavégzéshez használt informatikai rendszerekben.
- Magas üzemeltetési kockázat: a munkatárs adminisztrátor szintű jogosultsággal minden informatikai rendszerben, vagy jogosult ilyen hozzáférés állandó vagy ideiglenes beállítására.

A munkakörök, szerepkörök kockázati szintjeihez rendelt adatvédelmi és EIR üzemeltetési kockázatainak összerendelését az alábbi táblázat tartalmazza:

Munkakör, szerepkör kockázati szintje	Adatvédelmi kockázat	EIR üzemeltetési kockázat
Alacsony	Alacsony adatvédelmi kockázat	Nincs üzemeltetési kockázat
Közepes	Közepes adatvédelmi kockázat	Közepes üzemeltetési kockázat
Magas	Magas adatvédelmi kockázat	Magas üzemeltetési kockázat

3.1.3. FEGYELMI ELJÁRÁS

Amennyiben egy belső ellenőrzés során, vagy harmadik féltől, felettes hatóságtól kapott információk alapján felmerül a gyanú, hogy a munkatárs megszegte az informatikai biztonsági szabályzat előírásait, úgy fegyelmi eljárást kell lefolytatni.

A fegyelemi eljárás lefolytatásának lépései:

- vizsgálat: az informatikus és az érintett adatgazdák elvégzik a szükséges ellenőrzést és dokumentálják a tényeket, szakmai tanácsadással az informatikai biztonsági felelős segíti a munkát,
- értesítés: az érintett személyt a felmerült szabályszegés megállapítása után értesíteni kell a vizsgálatról és annak okáról,
- döntés, szankciók alkalmazása: a vizsgálat során készült dokumentáció alapján a jegyző, a szervezeti egység vezetője, az adatvédelmi tisztviselő és az informatikai biztonsági felelős meghallgatja a szabályt megszegő munkavállalót, és meghatározza az alkalmazandó szankciókat a szabályszegés súlyosságának, a belső szabályoknak, valamint a jogszabályoknak megfelelően,
- a fegyelmi eljárás eredményét szóban vagy írásban a jegyző közli a szabályt megszegő munkavállalóval.

A fegyelmi eljárás során alkalmazható szankciók:

- szóbeli figyelmeztetés: a szabályszegés nem veszélyezteti adatok bizalmasságát, sértetlenségét, rendelkezésre állását (pl: privát adatok tárolása a munkához használt eszközökön, fájltárhelyen, stb.).
- írásbeli figyelmeztetés: az adatok bizalmasságának, sértetlenségének, rendelkezésre állásának véletlen (ismeretek hiánya, figyelmetlenség, stb.) veszélyeztetése esetén, vagy 1-nél több szóbeli figyelmeztetés esetén; (pl: információk megküldése arra jogosulatlan személy részére, stb.)
- átmeneti hozzáférés-visszavonás, áthelyezés más alacsonyabb szintű munkakörbe, szerepkörbe: az adatok bizalmasságának, sértetlenségének, rendelkezésre állásának szándékos veszélyeztetése esetén, vagy 1-nél több írásbeli figyelmeztetés esetén; (pl: adatok szándékos törlése, bizalmas információk megküldése arra jogosulatlan személy részére, stb.).
- fegyelmi elbocsátás: az adatok bizalmasságának, sértetlenségének, rendelkezésre állásának szándékos veszélyeztetése, amellyel jelentős kárt okoz a szervezetnek (pl: adatok szándékos helyreállíthatatlan törlése, titkos információk vagy ügyfél adatok megküldése arra jogosulatlan személy részére, stb.).

A fegyelmi eljárás során a jegyző által kijelölt informatikus vagy adatgazda feladata jegyzőkönyvet készít, amely tartalmazza:

- a szükséges bizonyítékokat is, (képernyőképek, releváns reportok, stb.)

- a vizsgálatban, eljárásban résztvevő személyek (jegyző, a szervezeti egység vezetője, az adatvédelmi tisztviselő és az informatikai biztonsági felelős)
- a jegyzőkönyvben szereplő vizsgálati eredmény alapján meghozott szankció, döntés.

3.1.4. MUNKATÁRSAK INFORMATIKAI BIZTONSÁGI KÉPESÍTÉSI KÖVETELMÉNYEINEK MEGHATÁROZÁSA

Alapvető követelmény, hogy valamennyi munkatárs rendelkezzen a munkája ellátásához szükséges felkészültséggel.

A végzettségre, az alkalmazás feltételeire vonatkozó szakmai és jogi előírásokat a Hivatal SZMSZ-e tartalmazza.

A jogszabályok által előírt előzetes felméréseket, vizsgálatokat le kell folytatni az alkalmazásba vétel előtt.

A képesítési követelmények alapdokumentumai a munkaköri leírások, amelyek minden új munkakör létrehozásakor, illetve már meglévő munkakörök változásaikor szükségszerűen elkészülnek, ezért mindenkor az aktuális állapotot rögzítik.

3.2. INFORMATIKAI BIZTONSÁG OKTATÁSA

3.2.1. AZ OKTATÁS CÉLJA

A felhasználói képzések célja, hogy a felhasználók tájékozottak legyenek az informatikai biztonsági követelményekkel kapcsolatban, és tudatában legyenek a követelmények figyelmen kívül hagyásának következményeivel és veszélyeivel. Az oktatásnak ki kell térnie az informatikai biztonsági, adatvédelmi folyamatokra, szabályozásokra és az adatfeldolgozás célszerű módszereire ezzel csökkentve a biztonsági kockázatokat.

3.2.2. MUNKATÁRSAK INFORMATIKAI BIZTONSÁGI KÉPESÍTÉSI KÖVETELMÉNYEINEK MEGHATÁROZÁSA

Az informatikai biztonsági oktatásokat a jegyző által megbízott személynek kell megszerveznie. Az oktatáson részt kell vennie a Hivatal informatikai infrastruktúrát használó alkalmazottainak. A képzésnek ki kell terjednie a biztonsági követelményekre, azok megsértésének következményeire, a kapcsolódó törvényi és hatósági szabályzásokra, a Hivatalon belül használandó eljárásokra, információs folyamatokra. Tudatosítani kell az informatikai biztonsági eljárások folyamatait, a hozzáférési jogosultságokat, a szerzői stb. jogok figyelembevételét.

Alapvető követelmény, hogy valamennyi munkatárs rendelkezzen a munkája ellátásához szükséges felkészültséggel. E követelmény teljesítése érdekében a vonatkozó jogszabályok és a munkatársak vezetőinek igénye alapján meghatározandók a munkatársakra vonatkozó általános és speciális képesítési előírások. A munkatársak vezetőinek igényei alapján, a jegyző által megbízott személy állítsa össze a képesítési követelményeket, amely igények informatikai vonatkozásainál az informatikus véleményét figyelembe kell venni.

A jegyző felelőssége az informatikával, informatikai biztonsággal, adatvédelemmel foglalkozó, a Hivatal állományában lévő munkatársak szakmai képzésének biztosítása.

3.2.3. INFORMATIKAI BIZTONSÁGI OKTATÁSI/KÉPZÉSI TERVEK ELKÉSZÍTÉSE

Az informatikai biztonsági oktatás során az oktatandó témaköröket és területeket az Informatikai Biztonsági Felelős határozza. Az oktatási anyagokat évente felül kell vizsgálni, az oktatásokat évente meg kell tartani. Az informatikai biztonsági oktatás során figyelembe kell venni:

- a Hatóságtól, külső szervezetektől érkező biztonsági riasztásokat és releváns esetben be kell építeni az informatikai biztonsági tudatossági oktatás anyagába;
- a technológiai változásokat;
- a jogszabályi változásokat;
- szervezet felépítésében bekövetkezett változásokat;
- szervezeti egységek közötti együttműködést.

Az informatikai biztonsági színvonal fenntartása érdekében rendszeresen biztosítani kell az informatikai biztonsági oktatást és megfelelő szintű továbbképzést, ezért frissíteni kell a tananyagot és meg kell tartani az oktatást:

- az új alkalmazott felvételénél,
- a jogszabályi változás esetén;
- alkalmazott új munkakörbe kerülésénél
- új alkalmazások bevezetésénél,
- új technológia bevezetésénél,
- évente, minden informatikai rendszert használó munkatársnak.

Az informatikai biztonsági tudatossági oktatásnak legalább az alábbi, felhasználókra vonatkozó témaköröket kell tartalmaznia:

- jogosultságok igénylése,
- incidens kezelés,
- „tiszta asztal, tiszta képernyő"
- adatok védelme
- jelszó kezelés,
- adathordozók használata,
- mobil informatikai eszközök használata,
- távmunka biztonsági vonatkozásai.

Az adatgazdáknak, informatikusnak és a jegyző által kijelölt személyeknek részt kell venniük az alábbi témaköröket felölelő oktatásokon is:

- jogosultságok kezelése,
- incidens kezelés,
- üzletmenetfolytonosság kezelése.

Az informatikai biztonsági oktatás után visszaméréssel (pl: vizsga) kell meggyőződni az ismeretek elsajátításának sikerességéről. A vizsga előtt meg kell határozni a sikeres teljesítés minimum elvárt szintjét.

Amennyiben szükséges úgy a Hatóságtól, külső szervezetektől érkező biztonsági riasztások alapján soron kívül tájékoztatni kell a munkatársakat a felmerült biztonsági kockázatról, eseményekről. A tájékoztatás a jegyző által kijelölt személy feladata.

A Hivatalnál tapasztalt informatikai biztonsági, valamint adatvédelmi események alapján, ha szükséges a jegyző által kijelölt személy tájékoztatja a munkatársakat az informatikai biztonsági felelős útmutatása szerint.

3.2.4. INFORMATIKAI BIZTONSÁGI OKTATÁSOK, KÉPZÉSEK LEBONYOLÍTÁSA

Az informatikai biztonsági oktatás keretében kiemelt hangsúlyt kell fordítani a felhasználói tevékenységek felügyeletére és szabályozására, hiszen statisztikai adatok alapján az informatikai rendszerekben bekövetkező fennakadások, hibák legnagyobb részéért közvetve vagy közvetlenül a felhasználók a felelősek.

A képzés gyakorlati lebonyolításához a Hivatal informatikai rendszerének lehetőségei szerint kell eljárni.

Az oktatáson, illetve továbbképzésen való részvétel az informatikai rendszerek felhasználói számára kötelezőek. A résztvevők a megjelenést a jelenléti íven az aláírásukkal igazolják.

3.2.5. INFORMATIKAI BIZTONSÁGI OKTATÁSOK, KÉPZÉSEK NYILVÁNTARTÁSA

A külső oktatásokon, képzéseken való részvétel igazolása, a megszerzett képesítő okirat (bizonyítvány) bemutatása a jegyző által megbízott személynek, a beiskolázott munkatárs feladata. A jegyző által megbízott személy feladata a munkatársak által elvégzett külső és belső képzések, oktatások személyre lebontott nyilvántartása. A képzési dokumentumokat 5 évig meg kell őrizni.

3.3. FELHASZNÁLÓK KÖTELESSÉGEI

3.3.1. FELÜGYELET NÉLKÜL HAGYOTT SZÁMÍTÓGÉPEK

Ha a felhasználó szüneteltetni a munkaállomáson végzett tevékenységét, ki kell jelentkeznie, és zárolnia kell a számítógépet. Amennyiben nem jelentkezik ki, automatikus képernyővédőt kell alkalmazni, melynek **időzített aktiválása a munkaállomás kihasználatlansága esetén nem lehet több 15 percnél.** A rendszernek meghatározott idő után újra kell indítania az azonosítási és a jogosultság ellenőrzési folyamatot, a felhasználó csak az újbóli bejelentkezés, illetve jelszó megadás után folytathatja a munkát.

A munkaállomás őrizetlenül hagyásakor a felhasználó köteles zárolni a számítógépét (Windows + L) annak érdekében, hogy illetéktelenek ne tudjanak bizalmas információkhoz jutni a bejelentkezve hagyott számítógépen keresztül.

A megnyitott alkalmazásokat, a használatot követően a felhasználónak be kell zárnia.

A felügyelet nélkül hagyott munkaállomások védelmére vonatkozó beállításokat az informatikus végzi. A felhasználóknak tilos az informatikus által beállított paramétereket megváltoztatni.

3.3.2. RENDSZER-FÜGGETLEN MENTÉSI ELŐÍRÁSOK FELHASZNÁLÓK SZÁMÁRA

Az adatokat mindig a központi munkakönyvtárban kell tárolni.

Amennyiben nem központi mentéssel rendelkező tárterületre dolgoznak a Hivatal felhasználói (fájlszerver, alkalmazás központi adatbázisa), hanem saját munkaállomáson tárolnak, vagy dolgoznak fel adatokat, a felhasználók kötelezettek a következő szabályok betartására:

- Az adatokat mindig két különböző helyen kell tárolni (pl.: felhasználók saját munkaállomásai és központi szerver, vagy az informatikustól kapott titkosított külső adathordozó).
- Az irodai alkalmazásokban be kell kapcsolni és 10 percre állítani az automatikus mentési funkciót, és ettől függetlenül öt-tízpercenként kézzel is menteni kell.
- Az adatokat titkosítással is védeni kell a 9.1.4 Titkosítási előírások fejezetben leírtaknak megfelelően.

3.3.3. „TISZTA ASZTAL, TISZTA KÉPERNYŐ" POLITIKA

A következő szabályokat minden munkatársnak be kell tartania:

- az irodákat még rövid időre történő elhagyás esetén is zárni kell, amennyiben senki más nem tartózkodik bent;
- értekezletek végén a védendő, vagy kiemelten védendő adatokat tartalmazó dokumentumokat az értekezlet színhelyéről el kell távolítani;
- adatok faxon történő továbbításánál személyesen ellenőrizni kell mind a küldő, mind a fogadóoldalon, hogy illetéktelen személy nem férhet hozzá a dokumentációhoz;
- ha az adatok faxon kerülnek továbbításra, a fax rendeltetésszerű megérkezését telefonhívással kell ellenőrizni;
- az íróasztalon csak az adott munkafolyamattal kapcsolatos dokumentumok lehetnek, minden más dokumentumot el kell zárni;
- a nem használt adathordozókat (papír alapú és informatikai eszközök) el kell zárni;
- a számítógép „asztalán" csak a munkához szükséges alkalmazások parancsikonjai legyenek kihelyezve;
- a számítógépen csak azok az alkalmazások legyenek elindítva, illetve csak azok a dokumentumok legyen megnyitva, amelyek az adott munkafolyamat elvégzéséhez feltétlenül szükségesek;
- amennyiben egy dokumentumra a munkafolyamat során vagy a munkafolyamat befejeztével már nincs szükség, úgy azt a központi szerverre fel kell másolni, vagy fel kell tölteni az adatkezelő alkalmazásba és a számítógépről le kell törölni.

A munkahely elhagyásánál meg kell akadályozni programok és adatok illetéktelen használatát:

- Ki kell jelentkezni a nem használt és hitelesítést igénylő alkalmazásokból.
- Be kell zárni a megnyitott dokumentumokat.
- Jelszavas képernyővédőt kell alkalmazni a 3.3.1 Felügyelet nélkül hagyott számítógépek fejezetben leírtaknak megfelelően.
- El kell zárni a védendő és kiemelten védendő adatokat tartalmazó dokumentumokat, iratokat.
- Ki kell kapcsolni a számítógépet.

3.3.4. FELHASZNÁLÓK LOGIKAI HOZZÁFÉRÉSSEL KAPCSOLATOS KÖTELESSÉGEI, FELELŐSSÉGE

A felhasználóknak ismerniük kell a jelszavak, illetve a kezelésükben lévő berendezések használatára vonatkozó előírásokat.

A Hivatal informatikai rendszerének használatával kapcsolatos felhasználói feladatok, felelősségek:

- a felhasználói jelszavak titkosan kezelendők;
- a jelszó elfelejtése esetén a felhasználó az informatikustól igényelhet ideiglenes jelszót. Az ideiglenes jelszót az első bejelentkezés alkalmával kötelező megváltoztatni;
- a jelszó megválasztására, és a jelszavak kezelésére vonatkozó szabályokat a 6.1.3 Jelszómenedzsment fejezet tartalmazza;
- a jelszót a felhasználó semmilyen körülmények között nem jelenítheti meg a különböző adathordozókon, képernyőn, papíron stb. ;
- a jelszavak biztonságának megőrzéséért a felhasználó személyesen felel;
- a felhasználó a jelszavát nem oszthatja meg senkivel még ideiglenesen sem;
- a felhasználó köteles a jelszavát az előírt gyakorisággal és módon megváltoztatni.

Felhasználói jogosulatlan hozzáférés kísérlete esetén – a sikerességre vagy sikertelenségre való tekintet nélkül - a felhasználót felelősség terheli.

Minden, az informatikai rendszerek hozzáférésével kapcsolatos visszaélési kísérletet haladéktalanul jelenteni kell az informatikusnak, az ***Informatikai Biztonsági Eseménykezelési eljárásrendben*** megfogalmazottak szerint.

A felhasználó a számítógépre csak saját nevében és jelszavával léphet be, és az alkalmazásokat csak saját nevében használhatja.

4. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

Az objektumvédelem magában foglalja:

- az épületbe, helyiségekbe, a hozzájuk kapcsolódó területekre való belépés ellenőrzését,
- az illetéktelen behatolás megakadályozását,
- az épületben, helyiségekben, a területen való mozgás figyelését, ellenőrzését,
- a műszaki létesítmények, berendezések, al- és felépítmények állapotában bekövetkező változások megfigyelését, ellenőrzését,
- valamint a megfigyelések, ellenőrzések eredményeinek elemzése-értékelése alapján történő visszacsatolást (beavatkozást, korrekciót és a beavatkozás, korrekció érdekében igénybe veendő erőforrások folyamatos biztosítását).

4.1. BIZTONSÁGI ZÓNÁK

4.1.1. ALAPELVEK

A Hivatal tulajdonában és kezelésében lévő informatikai eszközök üzemképességének megőrzése érdekében minden, az eszközök működését veszélyeztető fenyegetettség ellen, annak bekövetkezési valószínűsége és az esetleges kárértéke függvényében megelőző- és ellenintézkedéseket kell kialakítani. A Hivatal jelentős informatikai eszközeit fenyegető főbb kockázati tényezők:

- áramkimaradás,
- túlmelegedés,
- tűzkár,
- lopás, szándékos károkozás,
- vízkár,
- természeti katasztrófa/előre nem látható katasztrófa (baleset),
- terrorizmus/katonai akció.

A kockázati tényezők és az azokhoz rendelhető megelőző és ellenintézkedések kapcsolatát az alábbi táblázat foglalja össze:

Kockázati tényezők és lehetséges megelőző ellenintézkedések	Szünetmentes tápellátás	Környezet monitorozása	Légkondicionálás	Tartalékeszközök	Tűzvédelem	Redundáns eszközök/telephely	Betörésvédelem
Áramkimaradás	■					■	
Túlmelegedés		■	■			■	
Tűzkár		■		■	■	■	
Lopás, szándékos károkozás				■		■	■
Vízkár				■		■	
Természeti katasztrófa						■	
Terrorizmus/katonai akció						■	

A követelménycsoportok feladatai:

- **Szünetmentes tápellátás:** biztosítsa az elektromos berendezés folyamatos áramellátását és ingadozásmentes feszültségellátását.
- **Környezet felügyelete:** jelezze az informatikai rendszer biztonságos működését befolyásoló környezeti paraméterek (hőmérséklet, páratartalom, a levegő por tartalma, víz, elektrosztatikus sugárzás) megengedett szinttől való eltérését, illetve megjelenését a helyiségben.
- **Légkondicionálás:** biztosítsa a helyiség optimális hőmérsékletét.
- **Tartalékeszközök:** biztosítsa a kieső eszköz azonnali pótlását.
- **Tűzvédelem:** jelezze a helyiségben lévő tüzet.
- **Redundáns eszköz/telephely:** biztosítsa az eszköz/telephely használhatatlansága esetén az elvárt szolgáltatások megfelelő szintű ellátását.
- **Betörésvédelem:** biztosítsa az eszközök fizikai biztonságát.

A biztonsági zónákra vonatkozó előírásokat, és a belépésre jogosultak nyilvántartását rendszeresen, évente legalább egyszer felül kell vizsgálni. Szükség esetén módosítani kell a szabályzatot, valamint a nyilvántartást.

4.1.2. BIZTONSÁGI ZÓNÁK KIALAKÍTÁSA

A biztonsági zónák kialakítása magában foglalja a Hivatal informatikai védelméhez szükséges építészeti, technikai és szervezeti intézkedéseket, valamint a különálló területeken lévő különleges

biztonsági követelményeket igénylő informatikai központok minden károsodással járó befolyás elleni védelmét.

A Hivatal informatikai rendszereinek fizikai védelme négy (a kárértékhez igazodó) biztonsági zónára tagozódik:

1. **Alap biztonsági zóna** – a Hivatal épületeinek belső területei;
2. **Kliens számítógépek zónája** – az alap biztonsági zónákon belül kliens számítógéppel ellátott helyiségek (irodák);
3. **Emelt szintű biztonsági zóna** – a Hivatal épületeinek azon helyiségei, ahol informatikai berendezések (hálózati eszközök,) kerültek elhelyezésre (informatikus irodája, az épületekben található hálózati eszközök helysége);
4. **Kiemelt biztonsági zóna** – az alap biztonsági zónákon belül fokozott védelmet igénylő helyiség: a központi szerverszoba.

A biztonsági zónák egymáshoz való viszonya:

4.1.3. BIZTONSÁGI ZÓNÁK VÉDELME

4.1.3.1. ÁLTALÁNOS BIZTONSÁGI INTÉZKEDÉSEK, KÖVETELMÉNYEK

Az informatikus feladata kezdeményezni, hogy a követelményeknek megfelelő biztonsági zónák kerüljenek kialakításra. A biztonsági zónák követelményeknek való folyamatos megfelelőségét (pl: ajtók zárva tartását) a jegyző vagy az általa megbízott személy évente legalább 2 alkalommal ellenőrzi, az eltéréseket írásban rögzíti.

Amennyiben a feltételek nem kielégítőek, úgy haladéktalanul gondoskodni kell a hiányosságok megfelelő kezeléséről.

A munkatársakat és az érintett harmadik feleket tájékoztatni kell a biztonsági zónák létezéséről és a hozzájuk kapcsolódó betartandó előírásokról. A biztonsági zónákban munkát végző felhasználó, vagy külső munkavállaló csak annyit tudhat meg a Hivatal informatikai rendszereiről és adatairól, amennyi a szerződésben meghatározott munka elvégzéséhez feltétlenül szükséges.

Az épületben ki kel alakítani a vészvilágítást, amely folyamatosan, az épület sérülése vagy áramszünet esetén is elegendő fényt biztosít az épület biztonságos elhagyásához.

4.1.3.2. BELÉPTETÉS BIZTONSÁGI ZÓNÁKBA, ILLETVE AZ INFORMATIKAI BIZTONSÁGI ZÓNAHATÁROKON

A Hivatal munkatársai kötelesek jelenteni a felettes vezetőnek, ha a belépésre jogosulatlan személy tartózkodik a Hivatal területén, illetve a be és kilépés ellenőrzése nem lehetséges vagy jogosulatlan belépési kísérletre utaló nyomokat találnak (pl. ajtó feszegetésre utaló nyomok). A belépéshez szükséges kódokat (riasztó, beléptető rendszer) rendszeresen évente legalább 1 alkalommal cserélni kell. A hitelesítő eszközök (riasztó, beléptető rendszer) kompromittálódása vagy elvesztése esetén azonnal cserélni kell őket. Beléptetőkártya elvesztése esetén a kártyát le kell tiltani, iroda vagy épület kulcs elvesztése esetén az érintett zárakat ki kell cserélni. A munkatársaknak a kulcsokról, beléptető kártyákról másolatot készíteni csak jegyző írásos engedélyével szabad. Az emelt szintű helyiségekbe történő belépést naplózni kell és a belépési naplókat rendszeresen legalább 3 havonta át kell vizsgálni. A gyanús belépéseket, belépési kísérleteket ki kell vizsgálni. A belépési naplókat és a belépési vizsgálatok eredményeit 1 évig meg kell őrizni.

Tartalékkulcsok, tartalék belépőkártyák kezelésének szabályai:

- egy tartalékkulcsot, vagy tartalék belépőkártyát, illetve riasztó vagy belépőkódot a jegyzői titkárságon kell elhelyezni lezárt, hitelesítéssel ellátott borítékban, vagy lepecsételhető kulcs dobozban,
- a tartalékkulcshoz, vagy a belépőkártyához, illetve tartalékkódhoz való hozzáférés csak naplózottan történhet, jegyző előzetes értesítésével és tudomásával, az engedélyezést utólagosan dokumentálni szükséges,
- a borítékon meg kell jelölni a felvételére jogosultak nevét és beosztását, kulcsdoboz esetén a használható pecsét számát,
- a boríték felnyitása után a kód használatát követően a kódot meg kell változtatni.

Kliens számítógépek biztonsági zónákba való belépés további szabályai:

- a zónába az ott dolgozó munkatársak jogosultak belépni, jogosultsággal nem rendelkező személyek belépését az iroda munkatársa engedélyezheti, vagy egy informatikus kíséretében tartózkodhat ott;
- a jogosultsággal nem rendelkező személyek magatartásáért és esetleges károkozásáért a kísérő személy a felelős;
- az irodák kulcsait csak az arra jogosultak tudják felvenni és leadni;
- a kliens számítógépek zónájába tartozó vagy attól magasabb biztonsági kategóriába sorolt helyiségeket zárva kell tartani, ha nem tartózkodik bent senki.

Emelt szintű biztonsági zónákba való belépés további szabályai:

- az informatikai területhez tartozó kulcsokat csak az arra jogosultak tudják leadni, illetve felvenni, a belépési jogosultságot jegyzői engedélyben kell dokumentálni;
- a kulcsok felvételekor ellenőrizni szükséges a felvételi jogosultságot;
- belépési jogokat rendszeresen felül kell vizsgálni, a szükséges változtatásokat el kell végezni, el kell távolítani azt a személyt, akinek a belépése nem indokolt;
- a zóna területén a jogosultsággal nem rendelkező személyek csak kísérő jelenlétében tartózkodhatnak;
- a jogosultsággal nem rendelkező személyek magatartásáért és esetleges károkozásáért a kísérő személy a felelős;

- a belépést az informatikus engedélyezheti, az engedélyt elegendő szóban megadni;
- a belépéseket fel kell jegyezni a ***Géptermi naplóba (10. számú melléklet)***.

Kiemelt biztonsági zónákba való belépés további szabályai:

- a zóna területén a jogosultsággal nem rendelkező személyek csak kísérő jelenlétében tartózkodhatnak, a belépést a jegyző engedélyezheti, az engedélyt elegendő szóban megadni.
- a kiemelt biztonsági zónába sorolt helyiségek esetén, a külsős, állandó belépésre jogosult személyek részére a belépést engedélyező névre szóló igazolványt kell kiállítani. Az igazolványt a belépésre jogosult személy köteles magánál tartani, kérésre felmutatni. Az igazolványt a tulajdonos át nem ruházhatja.
- a kiemelten védett területekre beléptető rendszert kell telepíteni,
- minden kiemelten védett területen történő, külső személy bevonásával végzett, tervezett munkavégzésről a munka megkezdése előtt 1 nappal, rendkívüli munkavégzésről (sürgős hibaelhárítás) a munka megkezdésével egy időben értesíteni kell az informatikust;
- meg kell győződni róla, hogy a kiemelten védett területre történő belépéskor, a munkát végző személynél csak a munkavégzéshez szükséges elektronikus eszközök találhatók;
- rendkívüli esemény bekövetkezésekor az informatikai területhez tartozó kulcsokat a jegyzői titkárságon, a jegyző által felhatalmazott személy veheti fel. Ezekben az esetekben a kulcsok felvételéről jegyzőkönyvet kell készíteni, mely jegyzőkönyvet az jegyzőnek el kell juttatni. Karbantartási tevékenység nem minősül rendkívüli eseménynek.

4.1.4. ALAP BIZTONSÁGI ZÓNA

A Hivatal épületeinek külső védelme biztosítja a biztonsági zónák megfelelő, teljes és homogén elkülönítését.

Elektromos, vagy fizikai (rács) védelmi eszközöket kell alkalmazni a nyílászárókon keresztül történő bejutás megakadályozása vagy észlelése érdekében, beltéri, vagy földszinti, illetve könnyen elérhető kültéri nyílászárók esetében egyaránt.

A növényzet nem nyújthat rejtőzködési és mászási lehetőségeket a homlokzaton lévő ablakoknál és más nyílászáróknál.

A biztonsági zónák területét a létesítményekkel együtt teljeskörű és homogén rendszerrel kell biztosítani.

Az átjárók mennyiségét és nyitva tartottságát a szükséges minimumra kell korlátozni.

A zónában csak nyilvános besorolású, tájékoztató dokumentumokat szabad elhelyezni.

A zónában tilos informatikai eszközök, jelentős vagy ettől magasabb biztonsági osztályba sorolt dokumentumokat tartalmazó szekrény vagy polc elhelyezése.

A zónában található informatikai hálózati csatlakozókat fizikailag ki kell kötni, ha nincsenek használatban.

4.1.5. A KLIENS SZÁMÍTÓGÉPEK ZÓNÁJÁRA VONATKOZÓ KÖVETELMÉNYEK

A 4.1.4 Alap biztonsági zóna fejezetben meghatározott biztonsági intézkedéseken és követelményeken felül az alábbi szabályozásoknak kell teljesülniük.

A kliens számítógépeket a lehetőségekhez képest, úgy kell elhelyezni az irodában, hogy:

- a monitor képét csak a számítógépet használó munkatárs láthassa a kívülről történő rálátás kockázata (pl.: nyílászárók felöli) minimális legyen,
- az kliens számítógép fizikailag ne legyen hozzáférhető az ügyfelek részére,
- nyomtatókat úgy kell elhelyezni a zónában, hogy ügyfelek ne férhessenek hozzá az eszközhöz, vagy a nyomtatóban található dokumentumokhoz.

A nyomtatókból a kinyomtatott dokumentumokat haladéktalanul el kell távolítani.

A kliens biztonsági zónába sorolt helyiségnek kell tekinteni azokat a helyiségeket, ahol nem nyilvános adatok feldolgozására alkalmazott informatikai erőforrások találhatók. A kliens biztonsági zónába legalább a következő helyiségeket kell sorolni:

- felhasználói irodák,
- tárgyalótermek.

4.1.6. EMELT SZINTŰ BIZTONSÁGI ZÓNÁKRA VONATKOZÓ KÖVETELMÉNYEK

A 4.1.5 A kliens számítógépek zónájára vonatkozó követelmények fejezetben meghatározott követelményeken felül az alábbi szabályozásoknak kell teljesülniük.

Az informatikai helységek kialakítása nem javasolt alagsorban vagy ez alatti szinteken. (vízkár esetén fokozott veszélynek vannak kitéve az eszközök)

A helyiségekben elhelyezett fizikai védelmi eszközök és érzékelők működését rendszeresen, évente legalább 1 alkalommal ellenőrizni kell.

A helyiségeket biztonsági zárral kell ellátni. Az eszközöket rack szekrénybe kell építeni. Az eszközök, kábelek legyenek ellátva jól felismerhető, a rendeltetésre utaló címkével.

A helyiségeket el kell látni mozgásérzékelővel és riasztóval. Az emelt szintű biztonsági zónákba sorolt helyiségnek kell tekinteni azokat a helyiségeket, ahol nem nyilvános adatok feldolgozására, tárolására alkalmazott kiegészítő informatikai erőforrások találhatók.

Az emelt szintű biztonsági zónákba a következő helyiségeket kell sorolni:

- a gerinchálózatot kiszolgáló aktív hálózati elemek elhelyezésére szolgáló helyiségek;
- Informatikus által használt raktár;
- Informatikus napi munkavégzésre használt iroda, helyisége;
- mentések végzésére szolgáló helyiségek.

4.1.6.1. TÁPELLÁTÁSSAL KAPCSOLATOS INTÉZKEDÉSEK

Az elektromos hálózat a hálózati eszközök és az eszközök menedzsmentjét, felügyeletét végző számítógépek vonatkozásában 30 perces áthidalási idejű, megszakításmentes átkapcsolással rendelkező szünetmentes tápegységgel legyen ellátva. A szünetmentes tápegységek hálózati betáplálása csak a Hivatal erre a célra kialakított elektromos hálózatáról történhet. Erre a hálózatra más elektromos fogyasztót rákapcsolni tilos.

A szünetmentes tápegységet úgy kell elhelyezni, hogy ahhoz eszközt csatlakoztatni vagy eltávolítani csak az informatikus tudjon.

Az informatikai rendszer eszközeinek üzemeltetéséhez lehetőség szerint külön elektromos hálózatot kell létrehozni. A hálózat terhelhetősége legyen nagyobb, mint amekkora terhelést a rácsatlakoztatott eszközök egyidejű használata okoz. Erre a hálózatra kizárólag csak az informatikai rendszerhez tartozó eszköz csatlakoztatható.

4.1.6.2. TŰZVÉDELMI INTÉZKEDÉSEK

A helyiségeket CO_2 tűzoltó készülékekkel kell ellátni, amelyeket a bejáratok előtt a falakon kell elhelyezni.

Minden éghető anyagot lehetőség szerint el kell távolítani a helységből.

A helyiséget el kell látni tűz és füst érzékelővel. A tűz és füst érzékelőnek értesítenie kell az épület üzemeltetőjét/gondnokát, a jegyzőt, valamint az informatikust.

4.1.7. KIEMELT SZINTŰ BIZTONSÁGI ZÓNÁKRA VONATKOZÓ KÖVETELMÉNYEK

A 4.1.6 Emelt szintű biztonsági zónákra vonatkozó követelmények fejezetben megfogalmazott követelményeken felül az alábbi szabályozásoknak kell teljesülniük.

Célszerű a szerverterem maximális szeparálását biztosítani és az ottani munkavégzést minimalizálni.

A szerverterem feladata elsősorban a szervergépek, hálózati eszközök biztonságos működésének biztosítása. Lehetőség szerint az informatikus irodájában kell elvégezni mindenféle lehetséges beavatkozást a szerverek konzolon keresztüli elérése segítségével.

Kiemelt szintű biztonsági zónákba a következő helyiségeket kell sorolni:

- központi szerver helyiség.

A szerverteremben kizárólag szerverek és hálózati eszközök tárolhatók, illetve ezek üzemeltetéséhez szükséges perifériák, kiegészítő eszközök.

A szerver-helyiségekben biztosítani kell az ott elhelyezett technikai eszközök, és a kábelezés áttekinthetőségét, logikus elrendezését.

Elektromos védelmi eszközöket kell alkalmazni a nyílászárókon keresztül történő bejutás észlelése érdekében.

A szerverterem ablakai legyenek védettek betekintés ellen. A betekintés elleni védelmet függöny, vagy védőfólia segítse. Az ablakok védelmét biztonsági ráccsal vagy betörésvédelmi fóliával biztosítani kell.

A szervereket és az archivált anyagokat tartalmazó helyiségekbe csak annak üzemeltetéséhez elengedhetetlenül szükséges közműhálózat csatlakozhat. A helyiségen belül nem mehet át víz, gáz, csatorna és egyéb közművezeték, felette és a határoló falfelületeken ún. vizes blokkot tartalmazó helyiségrész ne legyen. Amennyiben a közműhálózat kiváltása nem oldható meg, úgy gondoskodni kell a főelzárószelep hozzáférhetőségéről, amellyel a közműhálózat vész esetén teljesen elzárható. Kiemelt figyelmet kell fordítani a vízszivárgás monitorozására.

A jegyzőt értesíteni kell az informatikai központok területén érzékelt, különös jelentőséggel bíró egyéb események bekövetkezéséről (pl.: betörési kísérlet).

4.1.7.1. HŐMÉRSÉKLETRE, PÁRATARTALOMRA ÉS EGYÉB KÖRNYEZETI TÉNYEZŐKRE VONATKOZÓ INTÉZKEDÉSEK

A központi szerverszobát klimatizálni kell úgy, hogy az informatikai eszközök környezeti hőmérséklete működés közben 15-24 C°, tárolási hőmérséklete 0-40 C° között maradjon, a relatív páratartalom pedig ne haladja meg a 40%-ot.

A csak aktív vagy passzív hálózati eszközöket tartalmazó helyiségek esetén, amennyiben a helyiség hőmérséklete nem haladja meg a 40°C-ot, nem szükséges klíma alkalmazása.

A légkondicionáló berendezéseket lehetőség szerint úgy kell beállítani, hogy áramszünet után automatikusan visszakapcsoljanak.

A helyiséget el kell látni az alábbi érzékelőkkel:

- hőmérséklet érzékelő; (riasztási küszöb 25°C)
- víz és pára érzékelő. (riasztási küszöb páratartalom esetén 40%)

A szenzoroknak, a beállított határérték felett, automatikus riasztást kell küldeniük az informatikusnak.

4.2. BERENDEZÉSEK KARBANTARTÁSA, JAVÍTÁSA

4.2.1. A KARBANTARTÁS TERVEZÉSE, SZEREPLŐI

Az informatikai eszközökre vonatkozó rendszeres karbantartási munkákra karbantartási terv (***Karbantartási terv és napló***) elkészíttetése az jegyző feladata. A karbantartási tervben meghatározásra kerül a munkaállomások, szerverek, perifériák, hálózati eszközök fizikai és szoftveres állapotát ellenőrző karbantartások ütemezése, felelőse. A szoftveres karbantartásokat automatizált, jelentés készítésre képes rendszerrel támogatni kell.

Rendszeresen, évente legalább egy alkalommal felül kell vizsgálni a karbantartási terveket.

A karbantartási munkák szervezésénél figyelembe kell venni a berendezések gyártóinak előírásait, ajánlásait és az üzemeltetési tapasztalatokat.

Az informatikai eszközök rendelkezésre állásának biztosítása érdekében az informatikus szükség szerint, illetve tervezett és a felhasználókkal egyeztetett módon karbantartást végez.

4.2.2. A KARBANTARTÁS ÉS JAVÍTÁS SZABÁLYAI

Amennyiben a felhasználó az informatikai rendszer működésével kapcsolatosan hibát vagy rendellenességet észlel, azt köteles haladéktalanul bejelenteni az erre rendszeresített elektronikus felületen (helpdesk ticketing rendszer) az informatikus felé, aki a hibát haladéktalanul orvosolja.

A rendszeres karbantartás célja, hogy a Hivatal biztosítani tudja az ügymenethez szükséges eszközök és szolgáltatások zavartalan működését, hiba esetén az időben történő javítását. A rendszeres karbantartás során a karbantartásra jogosultaknak szükséges ellenőrizni a munkaállomások, szerverek, perifériák, hálózati eszközök fizikai és szoftveres állapotát, az esetlegesen felmerülő problémák megoldásáról gondoskodniuk kell.

A műszaki üzemeltetés, karbantartás és javítás feladatait az informatikus vagy – külön eseti megbízás alapján – erre feljogosított szervezetek látják el, illetve biztosítják.

Ha az eszköz meghibásodik, károsodik, értesíteni kell az informatikust, aki megállapítja a meghibásodás okát. Nem rendeltetésszerű használatból eredő hiba esetén jegyzőkönyvet kell felvenni, és egy-egy példányát meg kell küldeni az eszköz használójának és a jegyzőnek. Ha a kár az

eszköz nem rendeltetésszerű használatából következik be, felelősségre vonás a Hivatal irányadó belső szabályzatai alapján indítható.

Az informatikai rendszer egyes elemeinek karbantartását, javítását, szerelését csak olyan személyek végezhetik, akik a munkavégzésük során esetlegesen tudomásukra jutott titkos információk megőrzésére vonatkozóan titoktartási nyilatkozatot írtak alá, vagy a munkavégző személyt foglalkoztató vállalkozás – a megbízásából kiküldött személyre vonatkozóan is – titoktartási kötelezettséget vállalt.

A Hivatal informatikai berendezéseit kiszolgáló, illetve periféria típusú eszközeit (például szünetmentes tápegységek, nyomtatók, fénymásolók, faxok) csak az informatikus, vagy a jegyző által megbízott, arra jogosult személy tarthatja karban és javíthatja.

A karbantartást, vagy javítást végző szolgáltatók az emelt vagy kiemelt biztonsági zónába sorolt helyiségekben csak a munkavégzést engedélyező, a jegyző által megbízott személy felügyelete mellett tartózkodhatnak, dolgozhatnak.

Eseti távoli karbantartást, vagy hibajavítást csak erre szerződött Szolgáltató végezhet az informatikus felügyelete mellett, a jegyző jóváhagyása után. A távoli karbantartáshoz szükséges hozzáféréseket csak a karbantartás idejére szabad engedélyezni. A karbantartás befejezése után a hozzáférést le kell tiltani. Amennyiben az informatikai rendszerben beállítható a hozzáférést úgy kell létrehozni, hogy a rendszer a megadott időpontban automatikusan tiltsa le a felhasználó azonosítóját.

Távoli karbantartást, vagy hibajavítást felügyelet nélkül csak szerződött Szolgáltató végezhet. A karbantartást dokumentálni kell:

- a bejelentkezés pontos időtartamát,
- a bejelentkezés okát,
- elvégzett feladatokat.

A távoli karbantartást a jegyző, az adatgazdák vagy az informatikai biztonsági felelős ellenőrizheti. A távoli bejelentkezéshez kötelező a kéttényezős hitelesítés és a titkosított hálózati kapcsolat. A karbantartás elvégzése után le kell zárni a munkamenetet, ki kell jelentkezni az informatikai rendszerből.

A hálózat-karbantartási munkákat - mentések, szoftvertelepítés, eszközszerelés és mindazon rendszermenedzseri tevékenység, amely a hálózat üzemelését jelentősen lelassítja – munkanapokon a folyamatos munkarend zavarásának minimalizálásával vagy munkaidőn túl szabad elvégezni, a felhasználók egyidejű értesítésével, rendkívüli esetektől eltekintve.

Munkaállomást, laptopot javítás céljára csak abban az esetben szabad kivinni, ha nincs benne belső adattároló (merevlemez, SSD) vagy az adattároló teljes tárterülete titkosítással védett. Szervert, hálózati adattárolót (Storage, NAS eszközök), csak merevlemezek nélkül szabad javításra kiadni, vagy ezek nélkül kell leselejtezni. Kiemelten védendő besorolású adatokat tartalmazó javításra szoruló bármilyen merevlemezt (szerver, NAS, storage, stb. belső adattárolója is), szilárdtest alapú adattárolót (SSD, pendrive, memóriakártya) javításra kiadni TILOS, az ilyen merevlemezt le kell selejtezni, az 5.10.5 Adathordozók selejtezés fejezetben leírt szabályok szerint. Az adathordozók szállításának feltételeit az 5.10.3 Az adathordozók használatának, szállításának feltételei, követelményei fejezet tartalmazza.

A nyomtatók merevlemezén adattárolás nem történhet. Amennyiben történik adattárolás a nyomtatók merevlemezén, úgy azokat az eszközök elszállítása előtt le kell törölni, vagy ki kell szerelni. A nyomtatók merevlemezének tartalmát az informatikusnak elszállítás előtt ellenőriznie kell.

Az eszközök javítása után az informatikusnak ellenőriznie kell a javított eszköz működését, és adatbiztonsági ellenőrzést (vírusmentesség ellenőrzése, szoftver frissítés, stb.) kell végezni.

4.2.3. DOKUMENTÁLÁSI KÖTELEZETTSÉGEK

Az eszköz javítását, karbantartását, a feladatokat elvégző személynek egyidejűleg dokumentálnia kell (munkalap). A dokumentálás során fel kell tüntetni:

- feladatot végző személy nevét,
- feladat elvégzésének okát,
- dátumát,
- feladat mibenlétét.

4.3. ESZKÖZBIZTONSÁG

4.3.1. A SZERVEREKRE VONATKOZÓ ELŐÍRÁSOK

A szervereket a kiemelt biztonsági zónákban kialakított szerverteremben kell elhelyezni.

A szerverekre vonatkozó megfelelő környezeti feltételeket 4.1.7 Kiemelt szintű biztonsági zónákra vonatkozó követelmények fejezetbe foglalt előírások szavatolják.

A szerverek esetén a javítási munkákat helyben kell elvégezni. Ha az elszállítás elkerülhetetlen, a szerverek kiszállításához - mint minden informatikai eszköz kiviteléhez - a jegyző írásos engedélye szükséges és a **Hiba! A hivatkozási forrás nem található.**4.3.8 Felhasználói számítógépekre vonatkozó előírások fejezet rendelkezéseit be kell tartani. A karbantartási feladatokat a 4.2 Berendezések karbantartása, javítása fejezetben leírtak szerint kell elvégezni.

A szerverterem eszközeinek beállításait (mind hardver, mind hálózati alapbeállítások) aktuálisan dokumentálni kell. A dokumentálást az informatikus végzi.

4.3.2. HÁLÓZATI ESZKÖZÖKRE VONATKOZÓ ELŐÍRÁSOK

Az aktív eszközök fizikai védelmét a zárt adatelosztó (rack)szekrényekkel kell biztosítani.

Az aktív hálózati eszközöket legalább emelt biztonsági zónákban kell elhelyezni.

A folyosókon elhelyezkedő, informatikai eszközöket tartalmazó rack-szekrényben az aktív és passzív komponenseket úgy kell elhelyezni, hogy a patch kábelek rendezettek, és a rendelkezésre álló helynek megfelelő hosszúságúak legyenek. A rack-szekrények zárhatóságát és zártságát biztosítani kell.

4.3.3. BERENDEZÉSEK KÁBELEZÉSÉNEK BIZTONSÁGA

Az informatikai kommunikációs berendezések (pl. rack-szekrény) kábelezése rendezett, strukturált kialakítású legyen. A berendezések erősáramú kábelezését fizikailag el kell választani az informatikai-kommunikációs kábelektől.

A végpontokat számmal és felirattal kell jelölni és engedély nélkül tilos a meglévő hálózati vezetékek (UTP) áthelyezése más aljzatba.

A kábeleket a kábelrendező és a csatlakozó aljzatok között rögzített csatornában kell vezetni, a lengőkábelek nem keresztezhetnek közlekedési utat. A hálózat valamennyi elemét olyan környezetben kell elhelyezni, ahol a jogosulatlan fizikai hozzáférés megakadályozott.

4.3.4. EGYÜTTMŰKÖDÉSEN ALAPULÓ ESZKÖZÖK FIZIKAI VÉDELME

A Hivatal együttműködésen alapuló eszközeire vonatkozóan (pl: videókonferencia eszközök) az alábbi biztonsági előírásokat kell alkalmazni:

- az eszközök a bekapcsolt állapotukról egyértelmű visszajelzést kell adjanak, (pl: bekapcsolást jelző fény),
- az eszköz csak az arra jogosultak tudják fizikailag aktiválni,
- az eszközhöz csak arra feljogosított személy tudjon külső eszközt csatlakoztatni. (kamera, mikrofon, laptop, adathordozó, stb.)

4.3.5. A TELEFONKÖZPONTRA ÉS A RENDEZŐKRE VONATKOZÓ ELŐÍRÁSOK

A telefonközponthoz csak a telefonrendszer üzemeltetéséért felelős férhet hozzá.

4.3.6. FELHASZNÁLÓI SZÁMÍTÓGÉPEKRE VONATKOZÓ ELŐÍRÁSOK

Felhasználói számítógépet kizárólag csak az 4.1.5 A kliens számítógépek zónájára vonatkozó követelmények, vagy annál szigorúbb biztonsági követelményeknek megfelelő helyiségekbe lehet elhelyezni.

Az informatikai eszközök rendeltetésszerű használatáért a vagyonleltárban az eszköz használójaként kijelölt munkavállaló a felelős, vagy az a személy, aki felettes vezetői utasításra és engedéllyel azt használta.

Közös használatú eszköz esetén az eszközök rendeltetésszerű használatáért az a személy a felelős, akit a felettes vezető adott esetben kijelöl eszközök használatára.

A munkája során számítógépet használó felhasználó köteles az általa működtetett számítógépet és az ahhoz csatlakoztatott eszközöket:

- a rendeltetésnek megfelelően;
- munkavégzés céljából, szakszerűen, a Hivatal érdekeit szem előtt tartva az IBSZ által meghatározott módon használni;
- a munka befejezésével valamennyi eszközt kikapcsolni (kivéve akkor, ha ezzel ellentétes állandó, vagy egyedi írásos utasítást, illetve tájékoztatást nem kap).

Az informatikai eszközök használata során nem engedélyezett:

- az eszközt illetéktelen személynek átengedni;
- az eszköz közelében folyadékot, éghető anyagot, illetve felette, alatta vagy rajta az eszköz rendeltetésétől eltérő anyagot, tárgyat elhelyezni és tárolni;
- az eszközt a telepítési helyéről elmozdítani és elvinni az informatikus engedélye és közreműködése nélkül (kivételt képeznek a mobil eszközök).

Az informatikusnak a BIOS beállításait rendszergazdai jelszóval kell védeni módosítás ellen.

Az informatikai eszközökhöz bármilyen külső eszközt, illetve kábelt csatlakoztatni csak az informatikus engedélyével, vagy közreműködésével lehet. Az informatikus által már csatlakoztatott és beüzemelt eszköz további használata visszavonásig engedélyezett (pl.: fényképezőgép, nyomtató, stb.).

Az eszközök burkolatát megbontani TILOS. Alkatrészt csak az informatikus helyezhet be az eszközbe, illetve szerelhet ki az eszközből. A kliens számítógépeket az illetéktelen fizikai megbontás ellen védeni kell. Pl.: plombával

Címkét, jelölést, feliratot kizárólag a kijelölt informatikus helyezhet az informatikai eszközökre, illetve távolíthat el azokról.

Az informatikusnak a beállítások jogosulatlan megváltoztatása miatt keletkezett hibák esetén jegyzőkönyvet kell felvennie a nem megfelelő használat tényéről, majd a hibát el kell hárítania. A jegyzőkönyvet a gép használójának is alá kell írnia. A jegyzőkönyv egy példányát át kell adni a felhasználó felettes vezetőjének.

Minden informatikai eszközt használó munkatárs köteles az általa használt eszköz hibájának észlelésekor tájékoztatni az informatikust. Az informatikus intézkedik a hiba elhárításáról. Meghibásodás esetén – amennyiben a hibát nem tudja elhárítani, vagy a garanciális szerződések értelmében nem háríthatja el, értesíti a javítást végző szakmailag kompetens partnert és továbbiakban az 4.2 Berendezések karbantartása, javítása meghatározott módon járnak el.

4.3.7. ESZKÖZÖK KIVITELE

A Hivatal tulajdonában vagy kezelésében lévő informatikai eszközök kivitele a Hivatal területéről – az általános kiviteli engedélyezésen túl – jegyző által kiállított szállítólevéllel történhet. Az állandó vagy alkalmi kiviteli engedélyeket, illetve a szállítóleveleket a jegyző által megbízott személy tárolja.

Hordozható számítógépek állandó használatára jogosult személyeket a jegyző határozza meg.

Minden hordozható számítógéppel rendelkező felhasználó jogosult állandó jelleggel a Hivatal területén kívül is eszközét használni.

A tartósan a Hivatal területéről kikerülő eszközöket be kell vezetni a 2.1 Hardver- és szoftvereszközök nyilvántartása, kezelése fejezetben megjelölt módon.

4.3.8. ESZKÖZÖK VÉDELME IRODÁN KÍVÜL

A hordozható számítógépeket és az ahhoz kapcsolódó számítástechnikai berendezéseket szállító személyek:

- Kötelesek a számítógépet a szállítás idejére lehetőleg minél kevésbé szem előtt lévő módon elhelyezni.
- Hordozható számítógépeket TILOS a gépjárműben őrizetlenül hagyni!
- Azokban az esetekben, amikor az eszközöket nem a Hivatal tulajdonában lévő irodában (szálloda, lakás) kell hagyni, fokozott figyelmet kell fordítani a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása, vagy ellopása elleni védelemnek. Ha tartozékként rendelkezésre áll biztonsági rögzítő, akkor annak használata kötelező.
- Amikor a hordozható számítógépet vagy a hozzá csatlakoztatott pendrive-ot, mobil merevlemezes egységet nem használják, a mobil adathordozókat a hordozható számítógépből kivéve, attól elkülönítve, biztonságos helyen szükséges tárolni.
- Nem engedélyezett a gépet bármilyen indokolatlan veszélynek kitenni, az eszközt csak rendeltetésének megfelelően szabad használni.

4.3.8.1. A BERENDEZÉSEK BIZTONSÁGOS TÁROLÁSA

A tartalékberendezéseket, a kritikus rendszerdokumentációk, szoftverek törzspéldányait és a biztonsági adathordozókat a munkavégzés helyétől távoli és védett helyen kell tartani.

Az érzékeny adatokat tároló és feldolgozó eszközöket úgy ajánlatos elhelyezni, hogy a használat alatti rálátás kockázata minimális legyen.

A rendszer teljes életciklusa során gondoskodni kell az adott rendszerre meghatározott fizikai és környezeti biztonságról.

Biztosítani kell, hogy az informatikai rendszer kritikus elemeire maradéktalanul kiterjedjen a fizikai hozzáférés-ellenőrzés, amely így megakadályozza az illetéktelen hozzáférést a védett elemekhez.

Munkahelyről elszállított (kihelyezett) olyan eszköz, berendezés vagy tárgy (bármilyen számítógép, modem, mobiltelefon, fénymásoló, dokumentum stb.), amelyet - Hivatal felhatalmazása alapján - az irodán kívül használnak, egyenértékű biztonsági megítélés alá esik azzal, amelyet ugyanazon célra házon belül használnak, figyelembe véve azt a kockázatot, amit a Hivatal számára a házon kívül végzett tevékenység jelent.

4.3.9. MI A TEENDŐ, HA AZ ESZKÖZT ELTULAJDONÍTOTTÁK

Az eszköz használójának:

- Írásban jelenteni kell a számítógép eltulajdonításának tényét az informatikusoknak, és a jegyzőnek.
- Értesíteni kell a rendőrséget, és a rendőrségi jegyzőkönyvet el kell juttatni a jegyzőnek.
- Értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából, vagy a szálloda ingatlanján álló kocsiból lopták el.

Valamennyi rendőrségi és biztosítói jegyzőkönyvet, jelentést meg kell őrizni, és a jegyzőnek át kell adni.

5. A KOMMUNIKÁCIÓ ÉS ÜZEMELTETÉS IRÁNYÍTÁSA

5.1. AZ ÜZEMELTETÉSI ELJÁRÁSOK ÉS FELELŐSÉGI KÖRÖK

Az üzemeltetési feladatok meghatározása és karbantartása jegyző vagy az általa megbízott személy feladata.

Az üzemeltetési feladatokat tartalmazó dokumentumot (***Karbantartási terv***) rendszeresen, évente egy alkalommal, az informatikai környezet, vagy a karbantartáshoz használt eszközök megváltozásakor felül kell vizsgálni.

A ***Rendszerdokumentációban*** le kell dokumentálni, az informatikai rendszer karbantartásához használt szoftver eszközöket. A dokumentációnak tartalmaznia kell:

- eszköz karbantartási funkciója,
- a szoftverrel karbantartott eszközök, eszköz csoportok,
- szoftver verziószáma amennyiben releváns,
- szoftver elérhetősége, tárhelye.

A távoli karbantartó vagy diagnosztikai szoftvernek meg kell felelnie a Hivatal biztonsági követelményeinek:

- jelszó kezelés a 6.1.3 Jelszómenedzsment fejezet szerint fejezet szerint,
- felhasználói fiók kezelése a 6.1.7 Felhasználói hozzáférések típusa fejezetben foglalt „Névre szóló rendszergazdai hozzáférés" előírásainak megfelelően,
- kéttényezős hitelesítés kell alkalmazni,
- az informatikai rendszer és karbantartó, diagnosztikai eszköz megbízható, titkosított adatcsatornán kell kommunikáljon.

5.1.1. DOKUMENTÁLT ÜZEMELTETÉSI FOLYAMATOK

A rendszer napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése és hiba esetén az eszközök javítása.

Az informatikusnak ismernie kell a Hivatal rendszereszközeinek, operációs rendszereinek, adatbázisainak alkalmazói rendszereinek, és védelmi rendszereinek működését. Az informatikai rendszerek (hálózati eszközök, szerverek, nyomtatók, hálózati adattárolók, adatkezelő szoftverek, üzemeltetéshez használt szoftverek, vírusvédelmi szoftver) pontos beállításait le kell dokumentálni a ***Rendszerdokumentációban***. A ***Rendszerdokumentációt*** úgy kell elkészíteni, hogy abból a rendszer működőképesen visszaállítható legyen akár egy másik gyártó eszközén is.

Az informatikus meghatározza és ledokumentálja a Hivatal által használt informatikai rendszerek alapkonfigurációját. Az alapkonfiguráció dokumentálását minden eszköz típusra (asztali számítógép, szerver, laptop, mobil telefon, szoftverek, hálózati eszközök) el kell készíteni, és naprakészen kell tartani. Az alapkonfigurációnak tartalmaznia kell azokat az alapvető, egységes beállításokat, amiket az adott eszköz típusra egységesen be lehet és be kell állítani:

- számítógép esetén: BIOS jelszó, fix boot sorrend, boot sorrend választás letiltása, kötelezően elvégzendő konfigurációs beállítások, alapértelmezetten telepítendő szoftverek verziószámmal együtt,

- laptop esetén: BIOS jelszó, fix boot sorrend, boot sorrend választás letiltása, LAN/WLAN egyidejűleg nem használható, kötelezően elvégzendő konfigurációs beállítások, titkosítási beállítások, alapértelmezetten telepítendő szoftverek verziószámmal együtt,
- szerver beállítások: BIOS jelszó, fix boot sorrend, boot sorrend választás letiltása, kötelezően elvégzendő konfigurációs beállítások, alapértelmezetten telepítendő szoftverek verziószámmal együtt,
- hálózati eszközök esetén: kötelezően elvégzendő konfigurációs beállítások, NTP beállítás, SNMP beállítás, felügyleti rendszerbe bekötés, naplóelemző rendszerbe bekötés,
- mobil telefon beállítások: kötelezően elvégzendő konfigurációs beállítások, titkosítási beállítások, alapértelmezetten telepítendő szoftverek
- szoftverek: naplózás engedélyezése, technikai userek létrehozása, jogosultság csoportok létrehozása, titkosítási beállítások, tanúsítványok telepítése, szoftver működéséhez szükséges port, protokoll, szolgáltatás, kiegészítő szoftverek, rendszer hardver követelmények (CPU, RAM, tárhely, stb.).

Az informatikai rendszerek konfigurációját és a hozzá kapcsolódó dokumentációt, amely tartalmazza az alapkonfigurációk leírását is, rendszeresen, legalább évente egy alkalommal felül kell vizsgálni, és ha szükséges a módosításokat el kell végezni. Az informatikai infrastruktúra változásakor, hardver vagy szoftver eszközök cseréjekor vagy frissítésekor az alapkonfigurációkat tartalmazó dokumentációt felül kell vizsgálni, szükség esetén módosítani kell. A módosításokat úgy kell ledokumentálni, hogy a változások nyomon követhetők legyenek (dokumentumváltozás történet). A felülvizsgálat tényét le kell dokumentálni a ***Karbantartási terv és naplóban***. A dokumentum változás történetnek legalább az utolsó 10 verziót kell tartalmaznia, vagy 5 évre visszamenőleg meg kell lennie.

A rendszer felügyelete a felhasználói programok és adatbázisok, a szerverek és alapszoftverek és a hálózat működésének folyamatos figyelemmel kísérését kívánja meg.

5.1.2. VÁLTOZÁSKÖVETÉS, KONFIGURÁCIÓ KEZELÉS

Az informatikai rendszer védelmét (tűzfal, vírusvédelmi rendszer), alapvető működését és az informatikai rendszerek távoli elérését érintő változások alkalmazását az informatikai biztonsági felelős véleménye alapján jegyző engedélyezi. Az informatikai rendszer védelmével kapcsolatos konfiguráció változások esetén az informatikai biztonsági felelős véleményét ki kell kérni. A rendszerek beállításaival kapcsolatos bármely konfigurációs műveletet csak az informatikus végezheti. A konfigurációs beállításokat az informatikai biztonsági felelős szúrópróbaszerűen ellenőrzi.

A Hivatal informatikai rendszerei, csak a munkavégzéshez szükséges alkalmazásokat, szolgálatásokat tartalmazhatják.

A felmerült változtatási igényeket kielégítő beállításokat teszt környezetben az jegyző által meghatározott ideig, de legalább 1 héten keresztül, munkarendszerűen tesztelni és üzemeltetni kell.

A Hivatal munkaállomásain használt szoftverek (segédprogramok, adatkezelő alkalmazások) és operációs rendszerek esetében mindig az üzembiztosan telepíthető legfrissebb szoftver verziót kell egységesen alkalmazni.

A frissítések megjelenését követően haladéktalanul le kell tesztelni és alkalmazni kell a frissítéseket, ha üzembiztosan telepíthetők. A kritikus vagy biztonsági frissítéseket 1 hétig, minden más frissítést 2 hétig tesztelni szükséges a teljes informatikai rendszerre történő telepítés előtt. A tesztelés történhet a Hivatalnál éles környezetben használt számítógépek egy meghatározott részének bevonásával (2-5 db). Ebben az esetben gondoskodni kell a számítógépek rendellenes működését okozó frissítések azonnal eltávolításáról.

A szoftverek használata közben jelentkező hibát minden felhasználó köteles jelenteni az informatikusnak. A szoftver hibás működését az informatikusnak jeleznie kell a szoftver gyártója felé, és az 5.2 Rendszer tervezés és elfogadás fejezetben foglaltak szerint kell eljárnia.

Amennyiben a szoftver hibája vagy sérülékenysége nem javítható és a rendszer nem lecserélhető, úgy az ismert hiba vagy sérülékenység kihasználhatóságának kockázatát a minimális szintre kell csökkenteni (pl. a rendszer izolálásával) és le kell dokumentálni a sérülékenységet vagy hiányosságot és a meghozott ellenintézkedést a ***Rendszerdokumentációban***.

Szerverek és hálózati eszközök esetében az alkalmazott operációs rendszerek frissítéseinek mindig az üzembiztosan telepíthető legfrissebb verzióját kell alkalmazni az operációs rendszer hibáiból adódó kockázatok mérséklésének érdekében. Minden az operációs rendszer működését, konfigurációját érintő változás esetén az éles rendszerrel megegyező környezetben tesztelni kell a változásokat.

Az alkalmazói szoftvereken végzendő, azok bármely funkcióját megváltoztató művelethez az informatikus és az érintett adatgazda engedélye szükséges. Szükség esetén kockázatelemzést, sérülékenység vizsgálatot kell végezni a változtatás bevezetése, élesítése előtt. A verzióváltás és egyéb, jelentős beavatkozást igénylő változás elvégzéséhez az adatgazda engedélye szükséges.

A szerver és a hálózati eszközök tekintetében minden esetben adatmentést kell végezni az operációs rendszer frissítése, illetve a konfiguráció módosítása előtt.

Az informatikusnak évente legalább 1 alkalommal le kell mentenie minden hálózati eszköz konfigurációját. A konfiguráció mentéseket meg kell őrizni az adott eszköz selejtezéséig. A mentéseket dokumentálni szükséges a karbantartási naplóban.

Az informatikai rendszerekben, az azok fejlesztése és üzemeltetése során bekövetkező változások követésére ki kell alakítani a megfelelő változásmenedzsmentet.

Az informatikai rendszer tervezése, megvalósítása és üzemeltetése során felmerült összes változást, változáskövetési eljárással, az informatikusnak dokumentálnia kell.

Az informatikai rendszerek - és különösen a védelmi rendszer - összes dokumentációjára is érvényesíteni kell a változáskövetést.

5.2. RENDSZER TERVEZÉS ÉS ELFOGADÁS

5.2.1. FEJLESZTÉSI, TESZTELÉSI ÉS ÜZEMELTETLÉSI RENDSZEREK KEZELÉSÉNEK, VÉDELMÉNEK SZABÁLYAI

A Hivatal informatikai rendszereinek teljes életciklusában biztosítani kell a rendszer által elérhető maximális védelmet. Figyelemmel kell kísérni az adatbiztonságot érintő változásokat és szükség esetén javító intézkedéseket kell tenni.

Szoftver fejlesztéskor a tervezés előtt meg kell határozni a fejlesztésben résztvevő szereplők felelősségét, szerepét, feladatát.

Különbség van új szolgáltatás bevezetését célzó projekt és már létező szolgáltatáshoz kapcsolódó projekt esetében:

- Új szolgáltatás bevezetése esetében még nincs változáskezelés
- Létező szolgáltatás esetében az új módosítási igények jöhetnek az igény vagy hibalistából.

Mindkét esetben részletes szoftverfejlesztési tervet kell készíteni és az elkészült dokumentum alapján, szükség esetén biztonsági kockázatelemzést kell készíteni, amely tartalmazza a rendszert érintő fenyegetéseket. A ***Rendszerfejlesztésiterv*** dokumentumot a szoftver fejlesztésének menedzselésével megbízott személy készíti, az informatikussal közösen. Az elkészült dokumentumot az informatikai biztonsági felelősnek véleményeznie kell.

A ***Rendszerfejlesztésitervben*** a meg kell határozni, hogy a fejlesztés mely fázisában szükséges az informatikai biztonsági felelősnek és a fejlesztendő szoftver adatgazdájának ellenőriznie kell a fejlesztés állapotát, illetve a műszaki specifikációnak való megfelelést. Az ellenőrzést dokumentálni kell és eltérés esetén javító intézkedést kell megfogalmazni, vagy szankcionálni kell a fejlesztéssel megbízottat a szerződés / megbízás alapján.

A jegyzőnek kell előírnia, hogy mely változás végrehajtása előtt szükséges tesztelés, valamint meg kell határoznia a tesztelésben résztvevők körét, személyét az 5.2.7.1 Rendszerteszt és az 5.2.7.2 Felhasználói teszt fejezetekben foglaltak szerint. A véglegesített szoftverfejlesztési terv alapján kezdődhet csak meg a szoftverfejlesztés.

A fejlesztői és teszt tevékenységeket az éles üzemeltetői környezettől elkülönült környezetben szabad csak végezni úgy, hogy az ne veszélyeztesse az informatikai szolgáltatások működését. A fejlesztői környezetet a szoftver fejlesztésével megbízott személynek kell biztosítania.

Az informatikus vagy a jegyző által megbízott személy felügyeli a beruházásokat, a fejlesztéseket.

A beruházásokra, a fejlesztésekre, valamint a szoftverfejlesztések tesztelésére az informatikai biztonsági felelős javaslatot tesz, véleményezi azokat.

5.2.1.1. SZAKMAI KÖVETELMÉNYEK ÖSSZEÁLLÍTÁSA

Szakmai követelmények megfogalmazását követően az alkalmazásfejlesztést igénylő terület feladata az igényléskor benyújtott fejlesztési igény jelzése a szakmai követelmények pontos meghatározásával. A szakmai követelményeket leíró dokumentum elkészítése az igénylő szervezeti egység vezetőjének (illetve az általa kinevezett munkatársnak) a felelőssége.

Szakmai követelményeket tartalmazó dokumentumnak kötelező adattartalma:

- az igényelt fejlesztéssel szemben elvárt funkcionalitás ismertetése.
- a fejlesztésre vonatkozó (környezeti) korlátok bemutatása.
- a rendszerrel szemben támasztott szakmai követelmények.
- biztonsági követelmények.
- felhasználói követelmények.
- üzemeltetési követelmények.
- infrastrukturális követelmények.

5.2.1.2. INFORMATIKAI KÖVETELMÉNYEK ÖSSZEÁLLÍTÁSA

Ezek meghatározása után - a fejlesztéssel szemben támasztott felhasználói követelmények ismeretében - a fejlesztési feladat precíz specifikálása az alábbiak alapján lehetséges:

- a fejlesztési igény alapos megismerése, elemeinek, tevékenységeinek folyamatainak feltárása,
- a rendszer elemeinek, működésének leírása, elemzése,

- az információs rendszer részletes feltárása, megismerése,
- az információáramlás és feldolgozás elemzése,
- az információáramlás iránya és szükséges jogosultságai,
- az alkalmazni kívánt ki- és beviteli eszközök, módszerek meghatározása,
- a szükséges képernyő és nyomtatási formátumok, ki- és beviteli mezők meghatározása,
- a rendszerben tárolt adatok típusainak, formátumának, mérethatárainak meghatározása,
- az informatikai rendszer jogszabályok szerinti meghatározott biztonsági osztályának meghatározása, mely tartalmazza a rendszerben tárolt adatok típusán alapuló indoklást is,

Ezen feladatok elvégzése a fejlesztést igénylő szervezeti egység vezetőjének felelőssége. Az informatikai fejlesztési feladatnak az előző pontban meghatározottakon túl tartalmaznia kell a következőket is:

- a fejlesztés hardver szükséglete,
- a fejlesztés szoftver követelményei,
- dokumentációk adattartalmával és felépítésével kapcsolatos elvárások,
- szükséges erőforrások bemutatása,
- fejlesztési projekt ütemezése,
- a fejlesztés életciklusának meghatározása,
- rendszertervek adattartalmával és felépítésével kapcsolatos elvárások.

5.2.1.3. DOKUMENTÁCIÓKÉSZÍTÉS

A fejlesztett rendszerhez kapcsolódó dokumentációk elkészítése az adott projekt vezetőjének a felelőssége, külső fejlesztés esetén a külső vállalkozónak a feladata. Az informatikus csak abban az esetben veheti át üzemeltetésre a fejlesztett rendszert, ha a ***Rendszerfejlesztésiterv*** a következőket tartalmazza:

- műszaki leírás, amely tartalmazza a teljes rendszer felépítésére, működésére vonatkozó műszaki specifikációkat.
- az implementációs tervet, valamint a Teszt tervet is, amely részletesen leírja az átállás lépéseit, körülményeit, biztonsági követelményeit, szükséges erőforrásokat.
- üzemeltetési leírás, amelyek tartalmazzák a rendszer üzemeltetésére vonatkozó eljárásokat, rendszerindítás, - leállítás, biztonsági intézkedések, napi tevékenységek pontos leírását, továbbá mentés/visszaállítási leírás, katasztrófa elhárítási tervet, amely tartalmazza az adott rendszerre vonatkozó speciális feladatokat, igényeket.
- beállítási terv/leírás, amely a rendszer jogosultsági és egyéb beállításainak az átadás-átvételkori állapotát tartalmazza.
- felhasználói leírás, amely tartalmazza a felhasználók számára a rendszer rendeltetésszerű használatára vonatkozó használati utasításokat.
- oktatási anyag, amely tartalmazza a felhasználói és üzemeltetői feladatokhoz kapcsolódó oktatási anyagot, valamint a javasolt oktatási tervet.

A ***Rendszerfejlesztésitervet*** felül kell vizsgálni az informatikai környezet megváltozásakor, illetve 2 évente. A dokumentum felülvizsgálatát az informatikus végzi.

5.2.2. ADATVÉDELMI ELŐÍRÁSOK ÚJ RENDSZEREK FEJLESZTÉSE SORÁN

Új alkalmazás fejlesztése során az alábbi adatvédelmi előírásokat kell megkövetelni:

- regisztrált felhasználók esetén a felhasználói profil módosítását, törlését biztosítani kell,
- jelszavak kezelése a következő fejezetben megfogalmazott feltételek szerint: 6.1.3 Jelszómenedzsment
- az adatbázist vagy az adatbázisban tárolt adatokat titkosítva kell tárolni,
- jelszavakat csak kódoltan (titkosítva, vagy csak jelszó hash) lehet tárolni,
- belépéskor a beírt jelszó ne legyen olvasható a képernyőn,
- jogosultságok kezelését ki kell alakítani az 5.2.6 Felhasználói jogosultságok kezelése fejezetben, megfogalmazott feltételek szerint,
- naplózni szükséges legalább az következő eseményeket: felhasználók be és kilépése, adatok törlése, módosítása,
- deperszonalizáció megvalósítása: a megadott felétételek szerint törlésre kijelölt adatokat meg kell változtatni, hogy az adatok ne azonosítsanak egy konkrét személyt, illetve a törlésre kijelölt adatot ne lehessen egy konkrét személyhez kötni. (pl: bankkártyaszámnak csak az utolsó 4 számjegye látszódjon).

A titkosításra vonatkozóan be kell tartani a 9.1.4 Titkosítási előírások fejezetben megfogalmazott előírásokat.

5.2.3. A BEMENŐ ADATOK ÉRVENYESSÉGÉNEK ELLENŐRZÉSE

Az adatbeviteli hibák felismerésére és korrigálására céljából ki kell dolgozni azokat az eljárásokat, amelyek biztosítják a nem megfelelő adatok visszautasítását az adatok rögzítésekor.

5.2.4. FELDOLGOZÁS FELÜGYLETE, AZ ÜZENETEK SÉRTETLENSÉGÉNEK ELLENŐRZÉSE

Az feldolgozási folyamat csak hozzáférés-ellenőrzés mellett engedélyezett.

Az adatok feldolgozásához szükséges jogosultságokat rögzíteni kell, és a jogosultságokat rendszeresen ellenőrizni kell a 6.1.5 Hozzáférési jogosultságok nyilvántartása fejezetben leírtaknak megfelelően.

A bevitt adatok bizalmasságát, hitelességét és sértetlenségét, valamint a rendelkezésre állást biztosítani kell.

Az adatfeldolgozás során biztosítani kell a sértetlenséget olyan biztonsági funkciókkal, mint pl. ellenőrző összeg képzése, digitális aláírás vagy elektronikus pecsét.

5.2.5. A KIMENŐ ADATOK ÉRVÉNYESSÉGÉNEK ELLENŐRZÉSE

Hivatal informatikai rendszeréből származó adatok kiadását vagy azokhoz történő hozzáférést minden harmadik fél esetében (az adat minősítésétől függetlenül), csak az adatgazda engedélyezheti. Az engedély lehet eseti és határozott időre szóló.

5.2.6. FELHASZNÁLÓI JOGOSULTSÁGOK KEZELÉSE

A hozzáférés jogosultság menedzselésénél a hozzáférés-vezérlés elvét kell alkalmazni a következő hozzáférési jogokkal:

- olvasási jog (betekintés),
- írási jog (létrehozás, módosítás),
- törlési jog,
- végrehajtási jog.

A saját fejlesztésű, illetve az éles üzemeltetés közvetlen támogatására használt idegen rendszereknek mindenképpen, az egyéb célra vásárolt (nem kritikus) rendszereknek pedig lehetőleg alkalmasnak kell lenniük a hozzáférési jogok egyedi vagy csoport szinten történő megkülönböztetésére és szabályozására.

A jogosultsági rendszereknek támogatniuk kell a jogosultságok módosítását, átadását másik személynek, törlését és időleges korlátozását. Új jogosultság kiosztását, a jogosultság törlését vagy átmeneti felfüggesztését csak erre felhatalmazott informatikus vagy adatgazda végezhesse el.

A jogosulatlan hozzáférési kísérleteket rögzíteni kell a biztonsági naplóban, amelynek értékelését rendszerenként kijelölt személyeknek, rendszerenként meghatározott időközönként el kell végezni.

5.2.7. TESZT

A ***Rendszerfejlesztésiterv*** alapján elkészült fejlesztési feladat üzemeltetésre való átadás feltétele egy átfogó teszt végrehajtása, amit két fázisban kell megvalósítani. Rendszerteszt során a rendszer üzemszerű működését, működtethetőségét, a felhasználói teszt során pedig a fejlesztési igényben megfogalmazott elvárások minőségi teljesülését kell vizsgálat alá venni. A tesztelési módszertannak javasolt követnie az ISO9126 és az ISO12207 alkalmazásfejlesztéssel és teszteléssel összefüggő (6.4 Verification) fejezeteit.

A fejlesztői és teszt tevékenységeket az éles üzemeltetői környezettől elkülönült környezetben szabad csak végezni úgy, hogy az ne veszélyeztesse az informatikai szolgáltatások működését.

A tesztek végrehajtását, a kötelező dokumentumok adattartalmát a fejlesztéshez kapcsolódó Projekttervben kell definiálni.

A ***Rendszerfejlesztésiterv*** meghatározott feladatok elvégzéséről Teszt jegyzőkönyvet kell készíteni, amelyet a projektvezetőnek kell jóváhagynia.

5.2.7.1. RENDSZERTESZT

A jóváhagyott ***Rendszerfejlesztésitervben*** szereplő teszt terv alapján a szükséges teszteket el kell végezni. A teszteknek az alábbi területeket kell érintenie:

- integrációs teszt,
- teljesítmény teszt,
- terhelési teszt.

5.2.7.2. FELHASZNÁLÓI TESZT

Teszt végrehajtását a Műszaki leírásban szereplő felhasználói teszt-terv alapján kiválasztott felhasználónak kell elvégezni, és az elvégzett feladatokat dokumentálniuk kell a terv mellékleteként csatolt Felhasználói teszt jegyzőkönyvben.

5.2.8. RENDSZEREK BEVEZETÉSE

Üzembeállítás feltételei, új informatikai rendszerek, illetve meglévők új verziójának elfogadásának és átvételének minimális feltételei - melyek teljesülését az informatikus ellenőrzi - az alábbiak:

- átadásra kerül a telepítő készlet, forráskód, telepítő leírás, helyreállítási (roll-back) eljárás és rendszer dokumentáció egyértelmű verzióazonosítóval ellátva,
- felhasználói és üzemeltetői tesztek, beleértve a biztonsági tesztek megtörténtek,
- oktatások megtörténtek,
- kommunikáció a felhasználók felé megtörtént.

Az új rendszer, vagy rendszerösszetevő csak akkor vezethető be, ha az informatikai szabályzatoknak megfelel.

5.2.8.1. PRÓBAÜZEM

A teljes rendszer sikeres tesztje után a rendszert próbaüzembe kell állítani, amelynek keretén belül az igénylők megkezdik a rendszer rendeltetésszerű használatát. A próbaüzem során feltárt hibák kijavításáig és a sikeres elfogadási tesztig, de legalább 1 hónapig tart. Az elfogadási tesztről jegyzőkönyvet (Elfogadási teszt jegyzőkönyv) kell készíteni és eljuttatni a jegyzőnek jóváhagyásra.

5.2.8.2. ÉLES ÜZEM INDÍTÁSA

Igazolt próbaüzem után megtörténhet az Implementációs terv alapján az éles üzemre való átállás.

5.2.8.3. ÁTADÁS AZ ÜZEMELTETÉSNEK

A projekt során átadott eszközökről, alkalmazásokról, dokumentációkról Átadás-átvételi jegyzőkönyvet kell készíteni, és átadni az üzemeltetés képviselőjének. A feladatok elvégzése Teljesítési igazolás aláírásával kerül dokumentálásra.

5.2.9. KAPACITÁSMENEDZSELÉS

Az informatikus feladata, hogy évente felmérje a meglévő kapacitásokat és a várható kapacitás igényeket, illetve évközben nyomon kövesse az informatikai rendszerek kihasználtságát és a beszerzési időt figyelembe véve jelezze a jegyzőnek, ha kapacitásbővítésre van szükség.

A jegyző feladata, hogy az éves fejlesztési tervekbe beépítésre kerüljenek a jogos kapacitás igények, valamint a váratlan kapacitás hiány esetén intézkedjen a rendelkezésre álló kapacitások átcsoportosításáról vagy a kapacitások bővítéséhez szükséges beszerzések elindításáról.

5.3. VÉDELEM ROSSZINDULATÚ ÉS MOBIL KÓDOK ELLEN

A fejezet célja, hogy a Hivatal egészére tekintve megfogalmazásra kerüljenek a vírusfertőzés megelőzésére és mielőbbi detektálására, a fertőzés megszűntetésére vonatkozó szabályok és feladatok.

A vírusvédelem feladata a Hivatal informatikai rendszereinek, azaz a különböző operációs rendszerrel működő szervereknek, különféle munkaállomásoknak és hálózaton kívül üzemelő számítógépeknek a számítógép-vírusok elleni hatékony védelme. A védelemtől elvárható, hogy működjön együtt az internet böngésző alkalmazásokkal, és támogassa az elterjedt levelező klienseket is, valamint rendelkezzen központi management felülettel a rendszer egységes beállításainak kezeléséhez.

A vírusvédelmi rendszert a Hivatal minden számítógépére és mobil eszközére telepíteni kell, nem engedélyezett olyan eszközt az informatikai hálózathoz csatlakoztatni, amelyen nincs telepítve proaktív vírusvédelem.

5.3.1. ÁLTALÁNOS VÍRUSELLENŐRZÉSI TUDNIVALÓK

A vírusvédelmi rendszerek hatékonyságának legfontosabb összetevői:

- kellő gyakorisággal aktualizáltnak kell lennie, hogy felismerési hatékonysága maximális legyen,
- rendelkezik folyamatos gyártói támogatással az esetleges hibák javításához, illetve az új kártevők mintáinak vizsgálatához,
- a védelmi szoftvernek minden potenciális támadási ponton aktívan üzemelnie kell.

A fenti specifikációnak megfelelően a következő védelmi rétegek kialakítása szükséges:

- A munkaállomások ellenőrzése, mivel ezek jelentik a vírusok által megcélzott elsődleges támadási felületet. A víruskereső szoftvernek minden lehetséges bejutási pontot ellenőriznie kell (CD-ROM, hálózat, e-mail, pendrive stb.).
- A rendszerben működő fájl- és alkalmazásszerverek, tűzfalak, levelező szerverek másodlagos támadási felületet jelentenek. Védelmük jelentős redundanciát visz a rendszerbe, és feltétlenül szükséges. A telepített víruskeresőnek – a munkaállomásokon futó változathoz hasonlóan – minden lehetséges bejutási pontot ellenőriznie kell (CD-ROM, hálózat, e-mail, pendrive stb.), különös tekintettel a szerverek rendeltetésszerű használata közben fellépő adatforgalomra (pl. fájlok forgalmazása, levelezés stb.).
- Az internetes levélforgalmat vizsgáló levélszemét-szűrő eszköz.

A víruskereső rendszerek két alapvető működési móddal rendelkeznek: valós idejű (aktív), illetve offline (passzív) üzemmódban dolgoznak. A hatékony védelem alapvető követelménye mindkét működési mód párhuzamos használata.

A vírusadatbázisok frissítése a rendszer hatékonyságának szempontjából kritikus fontosságú, mivel az elektronikus hálózatok korában az új vírusok megjelenése és globális elterjedése között esetenként csupán néhány óra telik el.

A vírusvédelmi rendszer felhő alapú vírusvédelmét ki kell kapcsolni. A felhő alapú védelem a vizsgálathoz egy távoli, nem a Hivatal által kezelt szerverre küldi el a vizsgálandó dokumentum kódrészleteit. A dokumentum a kódrészletből / kódrészletekből nem állítható össze, de érzékeny információk kerülhetnek ki a Hivatal hálózatából.

A vírusirtók központi menedzsmentfelülete a felhőből is szabadon használható, mivel ezek csak rendszer konfigurálását biztosítják, érzékeny adatot nem tartalmaznak, és nem biztosítanak hozzáférést az adott számítógépen tárolt adatokhoz.

A vírustámadások elleni védekezés Hivatal szintű megtervezése, kialakítása, valamint a vírusadatbázisok rendszeres frissítésének megszervezése, az informatikus feladata.

Biztosítani kell a Hivatal egészére kiterjedő, rendszeres és folyamatos vírusvédelmet kereskedelemben kapható, kiterjedt referenciával rendelkező szoftverekkel. A frissítésről az informatikusnak folyamatosan gondoskodnia kell.

A kialakított rendszer monitorozása és működtetése az informatikus feladata:

- ellenőrzi a vírusvédelmi rendszerek rendszeres frissítését;
- listát készít a rendszeresen manuálisan frissítendő számítógépekről (pl. mobileszközökről, a nyilvántartás szerinti eszközöket frissíti, és a frissülés megtörténtét ellenőrizi a számítógépeken és a vírusvédelmi szoftver program nyilvántartásaiban);
- tájékoztatja a felhasználókat a vírusvédelmi eszközök működéséről;
- megvizsgálja a felhasználók jelzése alapján a vírusgyanús eseteket;
- elvégzi a vírusfertőzés bekövetkezése esetén a szükséges vírusmentesítési lépéseket;
- figyelemmel kíséri a vírusvédelem hatékonyságát.

5.3.2. VÍRUSVÉDELMI ELŐÍRÁSOK

A vírusvédelmi programok beállítása során – a megadott védelmi szint betartása mellett - törekedni kell a rendszerek optimális használhatóságára.

A Hivatal számítógépes hálózatához csak aktív és naprakész adatbázis frissítésekkel rendelkező vírusirtó alkalmazással ellátott számítógép csatlakoztatható.

A Hivatal informatikai eszközein egységes vírusvédelmi megoldást kell alkalmazni.

5.3.2.1. TELEPÍTÉS

A víruskereső rendszerek konkrét telepítésének megszervezése, és elvégzése az informatikus feladata, ennek eredményeképpen minden külső adat fogadására alkalmas munkaállomáson rendszeresen frissített vírusirtó programnak kell működnie.

Az újonnan rendszerbe állított, illetve újratelepített számítógépeken gondoskodni kell a víruskereső rendszer telepítéséről. Megfelelően friss vírusvédelmi rendszer nélkül szervert és munkaállomást üzembe állítani tilos!

Amennyiben az alkalmazott víruskereső rendszer erre lehetőséget ad, akkor a hálózaton keresztül központosítva felügyelhető változatokat kell telepíteni. A telepítéskor gondoskodni kell róla, hogy a hálózati adminisztráció során egyértelműen megkülönböztethetők legyenek a különböző gépektől érkező adatok (üzenetek, jelentések, vírusminták, stb.).

Az informatikus feladata a központosított menedzselés, vagy előkészített telepítőkészlet hiányában telepítéskor a szükséges konfiguráció beállítása. Az informatikusnak gondoskodnia kell arról, hogy a felhasználók önhatalmúlag ne csökkenthessék a vírusvédelmi rendszer működésének hatékonyságát és be kell kapcsolnia a vírusirtó alkalmazás konfigurációs felületének jelszavas védelemét.

A szerver és kliens számítógépeken a vírusvédelem programjait úgy kell installálni, hogy minden file-megnyitás, file-zárás, futtatható file indítása műveletet automatikusan ellenőrizzenek. Az ellenőrzés felfüggesztése tilos.

5.3.2.2. AKTÍV VÉDELEM

A vírusvédelmi rendszer fő komponense az aktív (tárrezidens, valós idejű) védelem, mely a számítógép működése során állandóan dolgozik. Feladata a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlen használat előtti vírusellenőrzése. Az aktív védelem kikapcsolása tilos!

Amennyiben a felhasználó a víruskereső program lefuttatása során vírust észlel, fel kell jegyeznie a vírus nevét, a fertőzött file nevét, a munkaállomása számát, és ezeket az adatokat jelenteni kell az informatikus felé, akik gondoskodnak a vírus további terjedésének megakadályozásáról, és – amennyiben a felhasználói gépen futó program automatikusan nem törölte – a vírus szakszerű kiirtásáról.

Az aktív védelem informatikus általi bármely okból történő kikapcsolása esetén a passzív védelem kiemelt jelentőségű, ezért az informatikus feladata a vírusvédelem megoldása (akár pl. hálózati kábel kihúzása stb).

A vírusirtó aktív védelmének beállításakor engedélyezni kell, hogy a vírusirtó automatikusan küldjön riasztást az informatikus email címére, amennyiben kártevőt észlel. Az informatikusnak a beérkező riasztást meg kell vizsgálnia, és annak eredményétől függően kell eljárnia.

5.3.2.3. PASSZÍV VÉDELEM

A passzív védelem feladata a teljes állományrendszer átvizsgálása, tekintet nélkül az állományok használatára. A vizsgálatot havonta 1 alkalommal lehetőség szerint automatikusan le kell futtatni. A vizsgálat automatikus futtatásának beállítása az informatikus feladata.

A rendszerbe kívülről bekerülő fájlokat (akár USB-n beérkező, akár az Internetről letöltött adatról van szó) felhasználás előtt vírusellenőrzésnek kell alávetni. A vírusirtót úgy kell beállítani, hogy lehetőség szerint automatikusan ellenőrizze az adathordozó illetve a fájlok tartalmát az alábbi esetekben:

- hordozható adattároló eszközök (pendrive, mobil merevlemez) csatlakoztatásakor,
- fájlok internetről történő letöltésekor,
- email megnyitásakor.

A vizsgálat automatikus futtatásának beállítása az informatikus feladata. Ha a vírusirtó nem képes automatikusan lefuttatni a víruskeresést a felsorolt események bekövetkezésekor, akkor a felhasználó feladata és felelőssége a keresés kézi indítása. A rendszerbe kívülről bekerülő adatokat (akár USB-n beérkező, akár az Internetről letöltött adatról van szó) felhasználás előtt vírusellenőrzésnek kell alávetni. A víruskereső programok munkaállomásokon történő lefuttatása automatikus, illetve a felhasználó is kezdeményezheti.

A passzív védelem futása több időt is igénybe vehet, mivel sok állomány ellenőrzését végzi. A víruskeresést megszakítani tilos.

5.3.3. FRISSÍTÉSEK

A víruskereső rendszerek frissítése két vonalon zajlik: a vírusadatbázisoknak, illetve maguknak a víruskereső motoroknak a frissítése. Általánosan a vírusadatbázisok frissítése lényegesen gyakoribb.

A víruskereső programok frissítéseit (vírusinformációs adatfájlok és motorok) célszerű az Interneten keresztül elvégezni. A hálózat tehermentesítése érdekében egy belső frissítő eszközre (szerver vagy munkaállomás) javasolt letölteni a szükséges frissítéseket. A klienseket úgy javasolt beállítani, hogy elsődlegesen a belső frissítő eszközről érjék el a frissítéshez szükséges adatfájlokat.

A víruskereső programok adatbázis frissítését úgy kell beállítani, hogy az automatikusan, naponta legalább 2 alkalommal megtörténjen. Ennek technikai kidolgozása és rendszerbe állítása az informatikus feladata.

A víruskereső rendszert fejlesztő cégektől érkező figyelmeztetésekre reagálva indokolt esetben azonnali kiegészítő vírusadatbázis-frissítés szükséges.

A harmadik fél számítógépein használt vírusirtók adatbázisának frissítéséről a számítógép tulajdonosának kell gondoskodnia.

5.3.4. VÍRUSFERTŐZÉS

A víruskeresők a fertőzés tényének kimutatása után a konkrét vírusok karakterisztikájától függően képesek a fertőzések eltávolítására.

Vírusfertőzés riasztás esetén a számítógépet azonnal el kell távolítani a hálózatról.

Amennyiben a fertőzés automatikusan nem távolítható el, úgy a fertőzött állományt törölni kell. Az állomány ún. kiterjesztésének megváltoztatásával annak tartalmára a rendszer következtetni nem tud, így a vírusfertőzés megállítható, a fájl vizsgálható. Másik megoldás a vírusok „karanténba" zárása, azaz a felhasználók által nem elérhető helyre történő mozgatása is, mely könyvtárhoz csak az informatikus férhet hozzá, és ő végzi el a további vizsgálatokat.

Amennyiben felmerül a gyanú, hogy az eszköz a vírus fertőzés eltávolítása csak részben volt sikeres, vagy a számítógépen rendszerfájljai megsérültek, úgy a számítógép teljes tartalmát törölni kell, és újra kell telepíteni.

5.4. BIZTONSÁGI MENTÉSI ELJÁRÁS

A mentési és visszaállítási eljárásokat az informatikusnak úgy kell kialakítani, hogy az üzemeltetett rendszerek előre nem látható esemény (katasztrófa, vagy hardver, illetve szoftver meghibásodása, emberi mulasztás) bekövetkezése után, szükség esetén helyreállíthatók legyenek, biztosítva a folyamatos. napi működést. Biztosítani kell, hogy az üzemidő kiesés, adatsérülés, adatvesztés minimális legyen. A mentésből a rendszerek, a szoftverkörnyezet beállításainak, valamit a tárolt adatoknak teljeskörűen visszaállíthatónak kell lenniük a mentés pillanatának állapotára. A mentéseket naponta, központi mentőszoftverrel kell végrehajtani.

A mentési rendet évente egyszer felül kell vizsgálnia az informatikusnak.

5.4.1. TERVEZÉSI LÉPÉSEK A HIVATAL INFORMATIKAI RENDSZEREINEK BIZTONSÁGI MENTÉSÉHEZ

Új mentési rendszer kialakításának, vagy a régi rendszer átalakításának **első lépése** a mentési rendszerterv – ***Mentési utasítás (9. számú melléklet)*** - meghatározása. A tervezésnél, mint környezeti

paramétereket figyelembe kell venni, hogy milyen okokból történhet adatvesztés, és melyik informatikai biztonsági esemény milyen gyakorisággal következhet be. Az informatikus készíti el az adott rendszerre vonatkozó mentési, archiválási dokumentációt, melyet a jegyző jóváhagy. Az alábbi felsorolás sorrendje egyben bekövetkezési valószínűséget is jelent, csökkenő sorrendben.

Káresemény bekövetkezhet:

- felhasználói hiba,
- hardver hiba (merevlemez),
- vírustámadás,
- betörés, lopás,
- természeti csapás stb. következtében.

A rendszerterv kialakításánál az informatikai rendszer sajátosságait és alapvető követelményeit megfogalmazó alábbi alapadatokat kell figyelembe venni:

- a rendszer mentendő adatainak mennyisége,
- a rendszer mentendő adatainak növekedési üteme,
- a rendszer adatainak változási sűrűsége,
- a rendszer felhasználóinak száma,
- jogszabályi követelmények,
- a hálózat átlagos és maximális sebessége,
- az adatok tárolási környezetének bonyolultsága, a környezet újraépítésének nehézségei.

A tervezés **második lépése** az adatok osztályozása a ***Biztonsági Osztályba Sorolási eljárásrend (1. számú melléklet)*** alapján, azaz annak meghatározása, hogy a rendszerben lévő adathalmazok milyen fontosak a szervezet számára. A mentendő adatok meghatározása után az informatikusnak kell a mentési rendszerterv alappilléreit meghatározni. A mentési alapkövetelmények a következők:

- mentési frekvencia, – a mentések sűrűsége,
- mentési eljárás, – központi mentés, mely a következő módszerek egyikével történhet:
    - teljes mentés,
    - inkrementális mentés,
    - teljes és inkrementális mentés kombinációja.
    - adatbázis kezelők esetében:
        - off-line mentés,
        - on-line mentés.
- mentő eszközök fajtája, típusa, mennyisége, elhelyezése.

Az **utolsó lépés** a mentési rendszerterv kialakításához meghatározni a mentés végrehajtását leíró következő paramétereket:

- a mentési időpontot,
- a mentések megőrzési idejét
- a mentési eljárást a rendszeren belül,
- a mentési időablakot,

- a mentő eszközök fajtáit.

A mentés ütemezését úgy kell kialakítani, hogy a mentés a munkafolyamatokat, a munkafolyamatok a mentési eljárást ne akadályozzák.

5.4.2. MENTÉSI ELŐÍRÁSOK A BIZTONSÁGI MENTÉSÉRT FELELŐS MUNKATÁRSAK SZÁMÁRA

A mentésekért az informatikus a felelős. Az informatikai biztonsági felelősnek kell a mentések dokumentumait ellenőriznie, és a biztonsági előírások használatát betartatni.

A mentéseket az éles szerverektől elkülönítve, külön épületben, de legalább külön helyiségben kell tárolni. A mentéseket tartalmazó tárhelynek jelszóvédettnek kell lennie, és csak a mentés idejére lehet hozzáférhető a mentőrendszer számára.

A rendszerekre vonatkozó ***Mentési utasításban*** (***9. számú melléklet***) definiálni kell a következőket:

- az adatmentéseket tartalmazó hardver paramétereket,
- az adatmentő szoftver neve, verziója, licenc mennyisége,
- az adatmentő script neve, típusa, elérési útvonala vagy a scriptet tartalmazó alkalmazás neve, script adatmentési funkciójának tartalma,
- a mentett rendszerek társítása az adatmentő szoftverekhez, scriptekhez,
- a konkrét mentési feladatok, mentési job-ok/taskok paramétereinek meghatározása
    - mentő szoftver neve,
    - mentett szerver neve,
    - mentés típusa (teljes mentés, különbözeti mentés, adatbázis export),
    - mentés megőrzési idő,
    - mentés rotációja (mikor kerül a korábbi mentés törlésre),
    - mentés ütemezése (nap, óra, perc),
    - mentési ablak (mennyi ideig tart a mentés),
    - mentéseket tároló eszköz,
    - mentések logikai helye (megosztott könyvtár, LUN, stb),
    - mentést tartalmazó állomány, vagy könyvtár nevének felépítése (ha fájl szintű a mentés pl zip fájlt készít a szoftver),
    - mentésinaplót, értesítés kapja (email cím).

A ***Mentési utasítás (9. számú melléklet)*** példányát zárható páncélszekrényben kell elhelyezni. A dokumentum létrehozásáért, tartalmának kialakításáért és őrzéséért az informatikus a felelős.

Az informatikus kötelessége meggyőződni arról, hogy a mentések hiba nélkül lefutottak-e. Amennyiben a mentés során hiba történt, a hiba okát fel kell deríteni és az okot meg kell szüntetni. A hiba okának megszüntetése után, vagy ha a hibajelenségre nem található ok és feltételezhető, hogy a következő mentés hiba nélkül lezajlik, a mentést meg kell ismételni. A mentés hibás lefutása esetén a hiba kijavítása után a mentést ismételten el kell végezni.

Az adatok — alkalmazások és fájlszerverek — mentését automatikusan kell indítani ***Mentési utasítás (9. számú melléklet)*** meghatározottak szerint.

5.4.3. OPERÁCIÓS RENDSZEREK, AKTÍV ESZKÖZÖK BEÁLLÍTÁSAINAK RENDSZER SZINTŰ BIZTONSÁGI MENTÉSE

A Hivatal informatikai rendszerében megtalálható aktív eszközök beállításainak és firmware-nek mentésére, valamint a szerverek operációs rendszerét érintő változás esetén az operációs rendszerek mentésére rendszerszintű mentést kell készíteni, melynek felelőse az informatikus.

A munkaállomások operációs rendszerét érintő változás esetén (pl: szoftver upgrade), az informatikusnak mérlegelnie kell, hogy szükséges-e és ha igen, milyen mértékű mentést kell készíteni az adott eszközről.

A rendszerszintű mentésekből egyszerűen és gyorsan visszaállítható az adott rendszer egésze, megtakarítva az installáció nehézkes és hosszú műveletét. A rendszerszintű mentés készítését erre alkalmas szoftverrel kell elvégezni.

5.4.4. DOKUMENTÁLÁS

A mentési tevékenységről a mentőrendszer mentési naplót készít, mely tartalmazza a mentés dátumát, állapotát, és szükség esetén egyéb megjegyzéseket. A mentés során észlelt rendellenességek esetén, a hiba elhárítása után a mentést meg kell ismételni.

A mentési naplót a jegyző által megbízott személy ellenőrizi. A naplókat lehetőség szerint automatizált szoftverrel javasolt vizsgálni, és a naplóelemző rendszernek email értesítést kell küldenie a hibás vagy sikertelen mentésekről.

5.4.5. ADATMENTÉSEK TESZTELÉSE

Az adatmentések megfelelősségét rendszeresen - évente legalább egy alkalommal tesztelni szükséges. A teszt adatok visszaállítását egy ideiglenes környezetbe kell elvégezni, és ellenőrizni kell az visszaállított adatok használhatóságát. A teszt befejezése után törölni kell a tesztkörnyezetet. A tesztet dokumentálni kell az alábbi adattartalommal:

- teszt kezdetének időpontja, résztvevői
- a tesztelni kívánt mentés adatai:
    - tesztelni kívánt mentés neve,
    - mentés ideje,
- a visszaállítás részletei:
    - visszaállítás típusa (teljes, részleges),
    - visszaállítani kívánt adatok megnevezése,
    - visszaállítás helye,
    - visszaállítani kívánt állapot időpontja,
    - visszaállításhoz használt szoftver visszaállítás lépései, képernyőképek.
- a visszaállított adatok tesztelése:
    - tesztelt fájlok, mappák, programok felsorolása,

- a visszaállított adatok ellenőrzésének lépései (fájl megnyitás, adatbázis tartalom ellenőrzés, programfuttatás ellenőrzés),
- képernyőképek,
- visszaállítás befejezésének időpontja

- teszt eredménye, befejezésének időpontja, észrevételek

A mentés visszaállításának kezdete és a mentés visszaállítás befejezésnek időpontja között eltelt időt össze kell hasonlítani a besorolási ívben meghatározott helyreállítási idővel (RTO). Ha a mentésből történő visszaállítás nem tudja teljesíteni az üzletmenet által elvárt időt, úgy ezt fel kell tüntetni a jegyzőkönyvben és el kell végezni a szükséges fejlesztéseket, felülvizsgálatokat.

A mentés tesztelését a jegyző vagy az informatikai biztonsági felelős ellenőrizi.

5.5. VISSZATÖLTÉSI, VISSZAÁLLÍTÁSI ELJÁRÁS

A fejezet célja a Hivatal informatikai rendszerének adathordozóin tárolt adatok visszatöltési, visszaállítási eljárásainak meghatározása.

5.5.1. ADATOK VISSZATÖLTÉSÉNEK, VISSZAÁLLÍTÁSÁNAK SZABÁLYAI

Az adatgazdák vagy az informatikus feladata az adott rendszerhez kapcsolódó mentések visszatöltését kezdeményezni a jegyzőnél.

Az adatok visszatöltését az adott rendszer üzemeltetésével megbízott informatikus vagy a szerződéssel rendelkező külső szolgáltató végezheti el az informatikus által meghatározottak szerint. A visszatöltést a jegyző engedélyezi.

Az egyedi felhasználók jogosultak saját munkakönyvtáraiknak adataira vonatkozó visszatöltést önállóan is kezdeményezni, az informatikusnál.

A felülírásból adódó adatvesztés megelőzése miatt, az adatok visszatöltése, visszaállítása általában nem végezhető el az adatok eredeti helyén, környezetében. Erre a célra az eredeti környezettel megegyező jogosultsági beállításokkal rendelkező ideiglenes környezetet kell létrehozni, és az adatok visszatöltését, visszaállítását ide kell végrehajtani. Az adatokat csak ezt követően szabad az eredeti helyre visszaállítani.

Speciális szoftverek segítik a különféle mentési, visszatöltési, visszaállítási eljárások használatát. Ezek a szoftverek általában operációs rendszer és adatbázis, valamint mentőeszköz függők. Kiválasztásukat a mentési rendszerterv részeként kell elvégezni.

A tranzakció alapú rendszerek esetén ez egyes tranzakciókat is helyre kell állítani.

5.5.2. VISSZATÖLTÉSHEZ, VISSZAÁLLÍTÁSHOZ SZÜKSÉGES PARAMÉTEREK KIJELÖLÉSE

A visszatöltéshez, visszaállításhoz, a feladatot végrehajtó informatikusnak az alábbi feltételeket kell vizsgálnia:

- a visszatöltendő, visszaállítandó adatok körét,
- a visszatöltendő, visszaállítandó adatok verzióját, forrását,

- a visszatöltés, visszaállítás helyét,
- a visszatöltés, visszaállítás időzítését.

A visszatöltendő, visszaállítandó adatokat és a visszatöltés, visszaállítás forrását azonosítani kell, ezzel egyértelműen meghatározzuk, hogy mikori adatok kerülnek visszatöltésre.

5.5.3. DOKUMENTÁLÁS

A mentések, archiválások felbontását, illetve felhasználását, valamint a visszatöltéshez, visszaállításhoz kapcsolódó paramétereket és a visszatöltés, visszaállítás végrehajtását minden esetben a feladatot végző informatikusnak a ***Karbantartási naplóban*** vagy a ***Katasztrófa elhárítási jegyzőkönyvben*** kell dokumentálnia.

5.6. ARCHIVÁLÁSI ELJÁRÁS

A fejezet célja a Hivatal informatikai rendszer szerverein tárolt adatok archiválási eljárásainak, az archivált adatok biztonságos kezelésének meghatározása.

Az archiválás rendszerfüggetlen mentés, amelynek célja a rendszer archiváláskori adatállományának hosszú távú megőrzése.

5.6.1. AZ ARCHIVÁLÓ RENDSZER KIALAKÍTÁSA

Az archiváló rendszer kialakításánál figyelembe kell venni a következő tényezőket:

- mekkora adatmennyiség kerül archiválásra, milyen időközönként,
- milyen az archiválandó adatok növekedésének üteme,
- mennyi ideig kell megőrizni az adatokat,
- mennyi a maximális visszakeresési idő,
- milyen formátumban érdemes az adatokat tárolni.

5.6.2. AZ ARCHIVÁLÓ RENDSZER MŰKÖDTETÉSE

Az archiválás az informatikus feladata. Az archiválást meghatározott időközönként, de legalább évente egyszer, illetve rendszer változtatások esetén el kell végezni. Az archívumokat, ha más jogszabály vagy belső szabályzat (pl: Iratkezelési szabályzat) másképp nem rendeli, 1 évig tárolni szükséges.

Az archiválás időpontjának meghatározása a jegyző feladata.

5.6.3. DOKUMENTÁLÁS

Minden archiválási folyamatot — a mentések dokumentálására előírt módon — rögzíteni kell a folyamatot végző informatikusnak az ***Archiválási naplóban (11. számú melléklet)***.

Az archiválási médiumok érthető, világos jelölését a mentésekre vonatkozó előírások betartásával kell megvalósítani.

Az archív anyagok megőrzése során figyelembe kell venni a jogszabályi, illetve az Iratkezelési Szabályzat előírásait.

5.7. A MENTÉSHEZ ÉS ARCHIVÁLÁSHOZ HASZNÁLT ADATHORDOZÓK TÁROLÁSÁNAK FELTÉTELEI

A tárolásra vonatkozó, az 5.10 Adathordozók kezelése fejezetben meghatározott biztonsági előírásokat, tárolási körülmények biztosítását (mágneses tér, hőmérséklet és páratartalom), be kell tartani.

Ha a mentett anyagok fájlmegosztáson tárolódnak, akkor az éles rendszerektől és a napi mentéstől független tárhelyre kerüljenek. (Pl külön NAS vagy storage eszköz)

Az archiváláshoz használt adathordozók tárolását úgy kell kialakítani, hogy azokhoz kizárólag a jegyző és az informatikus férjen hozzá.

A Hivatal elektronikus szoftvereinek telepítő készletei, illetve adatainak mentésére és archiválására használt adathordozói és eszközei (pl: NAS vagy storage eszköz), a mentés dokumentuma, a helyreállítást biztosító leírások:

- biztonságos módon, a mentés helyétől (telepítés helyétől) eltérő helyen elhelyezett tűzbiztos fémszekrényben;
- vagy a mentés helyétől (telepítés helyétől) különböző tűzszakaszban elhelyezkedő helyiségben tárolandók és az elhelyezésükre:
    - megfelelő mechanikai védelemmel (pl. ablakráccsal, biztonsági zárral) ellátott;
    - elektronikus védelemmel (riasztórendszerbe integrált, füst-, illetve hő érzékelővel) ellátott;
    - regisztrált kulcsfelvétellel hozzáférhető;
    - páratartalma a gyártó által a tárolásra előírt maximális értéket nem haladja meg;
    - közművezetékektől mentes helyiséget kell kijelölni.

Az adathordozók természetes fizikai romlása és elhasználódása következtében előálló biztonságcsökkenés miatt a működtetendő programokról és hasznos adatokat tartalmazó adathordozókról, ha az adathordozó megközelíti (élettartam -10%) a gyártó által javasolt felhasználási időtartamot, és az adathordozót nem lehet selejtezni, akkor másolatot kell készíteni.

A mentett adatokat titkosítással kell védeni a jogosulatlan hozzáférés ellen. A titkosításhoz használt kulcsokat, jelszavakat borítékban, a jegyzői páncélszekrényben kell őrizni.

5.8. HÁLÓZATBIZTONSÁGI ELJÁRÁS

A fejezet célja, hogy az informatikai rendszerek által használt hálózati szolgáltatásokhoz való hozzáférések szabályai rögzítésre kerüljenek, valamint meghatározásra kerüljenek a hálózati szolgáltatások által elérhető egyéb funkciók, az Internet, intranet és az elektronikus levelezőrendszer.

5.8.1. BIZTONSÁGI ELŐÍRÁSOK A HÁLÓZATI TERVEZÉS ÉS MŰKÖDTETÉS SORÁN

A kommunikációs rendszerek tervezésénél a topológia kiválasztásával is támogatni kell a funkcionalitást, a működőképességet és az elvárt rendelkezésre állást.

Az adatátviteli hálózatok rendelkezésre állásának követelményét az érintett szolgáltatás szerint kell meghatározni, a magas rendelkezésre állás és a védelem megfelelő biztosítása érdekében a központi hálózati eszközöket redundáns módon kell kiépíteni. Megelőző és szükséghelyzeti intézkedéseket kell hozni a hálózat egyes komponenseinek kiesése esetére.

A működésfolytonosság biztosításához, az interneten keresztüli használt kritikus szolgáltatások folyamatos eléréséhez, legalább a kritikus eszközök részére másodlagos internetkapcsolatot kell a biztosítania a Hivatalnak. (pl: mobil internetkapcsolat, telefonon megosztott internetkapcsolat, stb.)

Az adathálózatok védelme számos hálózat-biztonsági eszközzel és rendszertechnikai megoldással (izolált hálózat, üzenettovábbító szerverek alkalmazása, tűzfalak, távoli elérés tiltása, titkosítás stb.) valósítható meg. A biztonsági eszközök szakszerű alkalmazásával el kell kerülni, hogy a védelem csak az operációs rendszerek és az alkalmazások biztonsági megoldásaira háruljon.

A rendszer minden érintett elemének meg kell akadályoznia a kommunikációs csatornához történő illetéktelen logikai hozzáférést az alábbi technikai megoldásokkal amennyiben értelemezhető az adott rendszerre:

- legalább SHA256 titkosító algoritmus használata,
- IPSec kommunikációs csatorna,
- HSTS védelem.

A védelem kialakítása során kerülni kell az elavult, nem megbízható protokollok használatát. (pl: TLS 1.2-nél régebbi protokollok)

A hálózati csatlakozások számát a lehető legkevesebbre kell korlátozni.

A jelszavak védett formában, titkosítva kerüljenek továbbításra a hálózatokon. (pl: SSL)

A hálózati aktív eszközöket jelszóval kell védeni, a jelszót — amelyet csak informatikus ismer, — zárt borítékban informatikus által kezelt zárható szekrényben kell elhelyezni.

A hálózati aktív eszközök adminisztratív felületeinek biztonságos elérése érdekében, ha lehetséges, megbízható tanúsítványt kell telepíteni az eszközökre.

Az aktív eszközök beállításait az eszköz szoftverének frissítése vagy a konfiguráció módosítása előtt le kell menteni.

A tűzfal eszközt úgy kell bekonfigurálni, hogy az védelmet nyújtson a külső támadásokkal szemben (pl: túlterheléses támadás). Lehetőség szerint az eszköz tartalmazzon IDS/IPS védelmi funkciót és biztosítsa az alábbi védelmet:

- a rendszer képes legyen az internet felőli támadások minél teljesebb detektálására;
- a rendszer biztosítsa a hálózat belső elemei felől érkező támadások detektálását;
- a rendszer rendelkezzen előre kidolgozott akciótervekkel a legtipikusabb és legvalószínűbb támadások kezelésére;
- a rendszer biztosítsa az eseti támadás-elhárítási módszerek alkalmazását oly módon, hogy azok szabályozott körülmények között legyenek végrehajthatók.

Az informatikai rendszereken (szerver, hálózati eszközök) csak a rendszer által nyújtott szolgálatásokhoz nélkülözhetetlen portok lehetnek nyitva, minden más portot zárva kell tartani.

A Hivatal hálózatát önálló fizikai vagy logikai szegmensekre kell bontani, melyek között az átjárhatóságot le kell tiltani:

- management hálózat: csak a Hivatal informatikai eszközeinek üzemeltetéséhez szükséges adminisztrátori hozzáféréseit tartalmazhatja. (pl: hálózati aktív eszközök managament felülete)
- belső hálózat: a felhasználók által használt eszközök kommunikációs hálózata, csak a Hivatal saját, munkavégzéshez szükséges, védett eszközeit tartalmazhatja. (számítógépek, laptopok, szerver erőforrások, nyomtatók)

A belső hálózatot megfelelő logikai védelemmel is el kell látni. (pl: 802.1x) A belső illetve management hálózat esetén a címkiosztáskor az alábbi szabályokat be kell tartani:

- fix hálózati címet csak a kritikus eszközök kaphatnak,
- dinamikus hálózati címet maximum 12 órára kaphatnak az eszközök, ezt követően meg kell újítani,
- dinamikus hálózati címet lehet úgy kiosztani, hogy az eszköz fizikai címéhez fixen hozzá van rendelve egy hálózati cím. (MAC cím – IP cím összerendelés),
- a különböző hálózati szegmensekben eltérő címtartományt kell használni.

Logikailag elkülönített "vendég" Wifi hálózat létrehozható, ebben az esetben a Hivatalhoz tartozó laptopokat, munkaállomásokat stb. technikailag korlátozni kell az ehhez való csatlakozásban. A vendég hálózat esetén gondoskodni kell:

- a hozzáférési jelszó rendszeres, évenkénti cseréjéről,
- az elérhető internetes tartalmak szűréséről,
- a hálózatra csatlakozáskor meg kell jeleníteni a felhasználási feltételeket,
- a hálózati kapcsolatot 4 óra használat után le kell bontani, hogy a felhasználónak ismét be kelljen jelentkeznie a hálózatra.

A Hivatal területén a belső hálózat wireless (vezeték nélküli) kapcsolat kialakítása során legalább az alábbi védelmi megoldásokat kell alkalmazni:

- AES titkosítás,
- a csatlakozáshoz legalább 12 karakter hosszú jelszót kell használni, mely kisbetűt, nagybetűt és számot is tartalmaz,
- be kell kapcsolni a biztonságosabb WPA2/WPA3 Enterprise védelmet.

A belső hálózat vezeték nélküli kiterjesztése csak többtényezős hitelesítés kialakítása esetén lehetséges.

Az informatikai rendszer védelmét biztosító technikai megoldásokat úgy kell konfigurálni, hogy egy lehetséges biztonsági incidens érzékelése esetén automatikusan küldjön riasztást az informatikusnak és az informatikai biztonsági felelősnek. A riasztást úgy kell beállítani, hogy a riasztást tartalmazó üzenet az elérhető lehető legtöbb részletet tartalmazza a lehetséges támadásról.

Az informatikai rendszer védelmét biztosító technikai megoldásokat úgy kell konfigurálni, hogy:

- visszakövethető legyen a támadás folyamata (pl: naplózás),
- automatizáltan tudjon reagálni és védekezni a legáltalánosabb támadási formák ellen. (pl portscan, adathalászat, DDoS, stb.),
- a több helyről érkező információkat fésülje össze és egy felületen jelenítse meg az incidensben érintett valamennyi eszközt és folyamatot.

Idegen tulajdonú hordozható számítógépek csatlakoztatása a Hivatal belső hálózatához csak a jegyző írásos engedélyével történhet.

A Hivatal belső hálózatáról, fixen telepített informatikai eszközt csak az informatikus távolíthat el.

Idegen tulajdonú eszközök engedély nélküli csatlakoztatása esetén az informatikus köteles az eszközt a Hivatal hálózatából haladéktalanul eltávolítani, erről jegyzőkönyvet felvenni és értesíteni az jegyzőt.

A hálózat belső dokumentációjának ***(Rendszerdokumentáció)*** tartalmaznia kell a hálózat topológiai rajzát, valamin minden belső szolgáltatást. A dokumentációnak tartalmaznia kell a kívülről elérhető szolgáltatások technikai paramétereit. (forrás és cél IP cím, port, protokoll, alkalmazás)

A biztonságos név-cím feloldást biztosító eszközöket redundáns módon kell kiépíteni.

A nyomtatókban ki kell kapcsolni az önálló, peer-to-peer, wifi hálózat funkciót (Wi-Fi Direct szolgáltatás), a nyomtatókon csak a belső hálózaton keresztül szabad nyomtatni.

Az együttműködésen alapuló eszközöket egy önálló hálózati szegmensbe kell elhelyezni, és gondoskodni kell róla, hogy az eszközök távolról ne legyenek észrevétlenül aktiválhatók. Amennyiben az eszközök nem alkalmasak a távoli észrevétlen aktiválás megakadályozására, akkor az eszközt le kell választani a hálózatról vagy ki kell húzni az elektromos áramból amikor nincs használatban.

5.8.1.1. INTERNET ELÉRÉSSEL KAPCSOLATOS SZABÁLYOK, BIZTONSÁGI ELŐÍRÁSOK

A Hivatal belső hálózatát tűzfallal kell leválasztani az Internettől. Valamint csak egy központi Internet kapcsolat engedélyezett a hálózaton. Több Internet kapcsolat egyidejű létesítése TILTOTT a Hivatal hálózatán és a Hivatal eszközein, ezért kliens eszközöket úgy kell beállítani, hogy egyidejűleg ne lehessen a vezetékes és vezeték nélküli hálózathoz is csatlakoztatni.

Az internetes elérést a felhasználói alkalmazások logikai hozzáférésének megfelelő módon kell kezelni.

A Hivatal területén külső (nem a Hivatal által felügyelt) wireless (vezeték nélküli hálózati) eszközhöz csatlakozni tilos.

Az Internet forgalmat az Informatikusnak naplóznia kell, de a naplók kizárólag az informatikai biztonsági incidensek okainak és felelőseinek meghatározására használhatók fel.

A Hivatal fenntartja a jogot, hogy az erőforrások védelme és a jogszabályi megfelelés érdekében hozzáférhetetlenné tegye egyes Web helyek látogatását és bizonyos állomány típusok letöltését. A tiltott weboldalak kategóriáit és a tiltás beállítását a jegyző utasításban rendeli el (***URL szűrési utasítás)***. A jegyző utasítás szerinti technikai korlátozás beállítása az informatikus feladata.

5.8.1.2. AZ INTERNET HASZNÁLATÁVAL KAPCSOLATOS SZABÁLYOK, BIZTONSÁGI ELŐÍRÁSOK

A szakmai feladatok hatékony ellátásához szükséges információkhoz, szolgáltatásokhoz való hozzáférés érdekében a Hivatal valamennyi felhasználója jogosult a munkahelyi internet, intranetes portál és elektronikus levelezés használatára. Az internet szolgáltatásait kizárólag munkahelyi eszközökön és csak a munkaköri feladatok ellátásához lehet igénybe venni, személyes célokra nem.

Tilos olyan tevékenységet folytatni, amelynek célja vagy előrelátható következménye a Hivatal hálózatának vagy szoftverintegritásának bármelyfokú és természetű megsértése.

Az internet elérését biztosító szoftverek beállításait tilos a munkaállomásokon megváltoztatni, erre csak az informatikus jogosult.

Az internet munkahelyi használata során nem engedélyezett:

- futtatható programok illegális letöltése,
- a programok védelmi rendszerét megkerülő alkalmazások letöltése, használata (kulcsgenerátorok, programtörések, exploitok)
- jogdíjas termékek illegális letöltése, másolása, tárolása, továbbítása és telepítése,
- a mindenkor hatályos jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése, tiltott haszonszerzésre irányuló tevékenység, szerzői jogok megsértése,
- profitszerzést célzó üzleti célú tevékenység és reklám,
- a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése,
- a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásokat indokolatlanul igénybe vevő tevékenységek,
- az eszközöket internetes számítógép erőforrás megosztásokhoz, elosztott számításokat végző alkalmazásokhoz használni, (pl: kriptobányászat, jelszófejtés, stb.)
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások – akár tesztelés céljából történő – túlzott mértékben való szisztematikus próbálgatása,
- a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítása, megrongálása, megsemmisítése vagy bármely károkozásra irányuló tevékenység,
- másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység,
- hálózati üzenetek, hálózati eszközök hamisítása.

Felhasználók internet használatára vonatkozó általános szabályok:

- csak a munkavégzéshez, szakmai tájékozottság bővítéshez információt, segítséget nyújtó oldalak látogathatók,
- mindig szem előtt kell tartani a Hivatal érdekeit és a törvényi és a belső szabályok által szabott határokat,
- az Internetről csak a munkavégzéshez szükséges adatállományok tölthetők le.

Tilos önhatalmúlag tesztelni a biztonsági mechanizmusokat, működésüket.

Tilos tudatosan kihasználni az esetleges előforduló szoftver hibákat, védelmi hiányosságokat.

Az Internet munkahelyi használatára vonatkozó előírások megsértéséből eredő károkért a károkozó kártérítési felelősséggel tartozik.

Az interneten (fórumon, közösségi oldalakon, üzenetküldő alkalmazáson, stb.) tilos publikálni bármilyen, a Hivatallal kapcsolatos nem nyilvános információt.

5.8.2. A HIVATAL INTERNETES HONLAPJA, KÖZÖSSÉGI OLDALA

A Hivatal a széleskörű tájékoztatás, gyorsabb információszolgáltatás, valamint tevékenységének bemutatása érdekében honlapot és közösségi oldalt üzemeltet.

5.8.2.1. A HONLAP ÉS KÖZÖSSÉGI OLDAL MŰKÖDTETÉSÉNEK SZEMPONTJAI

Működtetésekor az alábbi szempontokat kell figyelembe venni:

- tükrözze a Hivatal céljait,
- folyamatosan karbantartott, friss információkat tartalmazzon,
- az információk áttekinthetők és kereshetők legyenek,
- az anyagok és szolgáltatások folyamatosan elérhetőek legyenek,
- a tárolt információ és a szolgáltatások védve legyenek külső és belső támadások ellen.

A Hivatal honlapját és közösségi oldalát kommunikációs tevékenysége részének kell tekinteni, hiszen tartalma és szolgáltatásai befolyásolják a Hivatalról kialakuló belső és külső képet.

5.8.2.2. BIZTONSÁGI FELADATOK, FELELŐSSÉGEK

Nem publikálható szerzői jogi oltalom alá tartozó anyag, kivéve, ha a szerző írásos engedélyt adott.

A Hivatal informatikai rendszeréről és eszközeiről csak a jegyző által kijelölt személy szolgáltathat a jegyző által jóváhagyott adatokat.

A személyiségi jogok védelmében nem publikálható az emberi erőforrásokkal kapcsolatos bármilyen nem nyilvános információ, személyes adat (pl. otthoni lakcím, telefonszám stb.).

Tilos az Interneten publikálni a Hivatal informatikai rendszerére vonatkozó bármilyen információt, amennyiben a törvényi előírás nem rendelkezik másképp.

Tilos jogszabályba ütköző, vagy a jó ízlést és közerkölcsöt sértő tartalmat közzétenni.

A Hivatal weboldalára és közösségi oldalára csak engedélyezett, csak a Hivatal tevékenységével összefüggőtartalom tölthető fel. A weboldal vagy a közösségi oldal tartalmát csak a jegyző által arra feljogosított személy módosíthatja. A feladat ellátáshoz szükséges, az adatok kezelésére vonatkozó oktatásról, vagy képzésről a jegyzőnek, 2 évente gondoskodnia kell.

Rendszeresen felül kell vizsgálni valamennyi publikusan elérhető informatikai rendszer tartalmát, és a nem nyilvános, valamint a jogalap nélkül publikált információkat el kell távolítani. A felülvizsgálatot a jegyző által megbízott személy köteles 3 havonta elvégezni.

A Hivatal weboldalának és közösségi oldalának kialakításakor figyelembe kell venni a biztonsági szempontokat. A weboldal és a közösségi oldal adminisztrátori felületéhez hozzáférni csak felhasználónévvel és jelszóval történő hitelesítés után lehet. Célszerű a weboldal védelmét kiegészíteni tanúsítvánnyal. Amennyiben szükséges a weboldal és közösségi oldal szerkesztéshez különböző jogosultsági szinteket kell kialakítani.

A weboldal mappastruktúrájának jogosultság beállításait a weboldal élesítése előtt ellenőrizni kell, és csak a weboldal megfelelő működéséhez szükséges jogosultságokat szabad beállítani. A működéshez szükségtelen könyvtárakat le kell törölni.

A weboldal biztonságos működéséről rendszeresen, legalább kétévente meg kell győződni, technikai felülvizsgálat keretében. A vizsgálatot az jegyző által megbízott harmadik fél végzi a szerződésben rögzített feltételeknek megfelelően. A sérülékenységvizsgálati jelentés kiértékelésébe, a javító intézkedések meghatározásába be kell vonni az informatikai biztonsági felelőst.

5.8.3. AZ ELEKTRONIKUS LEVELEZÉS ELŐÍRÁSAI

Az elektronikus levelezés a Hivatal informatikai szolgáltatása, mely lehetővé teszi, hogy a hálózat egy felhasználója egy másik felhasználó számára elektronikus levelet, üzenetet küldjön.

A belső munkatárs az általa használt munkaállomásáról a Hivatal levelezőrendszerének megfelelő levelezőklienssel kapcsolódik az email kiszolgálón lévő postaládájához, ezen keresztül küldhet leveleket, illetve olvashatja el a beérkező üzeneteket.

A Hivatal minden munkatársának egyedi e-mail címet biztosít a Hivatal az alábbi névkonvenció alapján:

- vezetéknév.keresztnév@kenderes.hu,
- szervezetiegyseg@kenderes.hu.

A Hivatal dolgozóinak a Hivatalnál szabványosított és az informatikus által telepített levelező szoftvert kell használnia, ezen keresztül küldhet leveleket, illetve olvashatja el a beérkező üzeneteket.

A Hivatal informatikai rendszere és adatai védelmében a leveleket vírus ellenőrzésnek kell alávetni. Minden kimenő és bejövő levélen szűrés történik, melynek során ellenőrzésre kerül, hogy a levél tartalmaz-e vírust.

A Hivatalnak joga van az e-mail forgalom archiválására. Kivételes esetben a jegyző írásban rendelheti el a felhasználók levelezésébe történő betekintést. Az eljárást dokumentálni szükséges az indokok, a hozzáférés időpontjának, a megtekintett postafiókok és érintett felhasználók, valamint a betekintésre feljogosított személy nevének feltűntetésével.

Az elektronikus levelek személyes adatokat is tartalmazhatnak, ezért az e-mail adatbázisok védelmét a személyi adatokra vonatkozó szabályok alapján kell kialakítani.

Az elektronikus levelezés kialakításának szempontjai:

- megfelelő felhasználó azonosítás,
- felhasználókénti tárméret korlátozás,
- titkosítás alkalmazása.

5.8.3.1. A FELHASZNÁLÓ ELEKTRONIKUS LEVELEZÉSRE VONATKOZÓ JOGAI ÉS KÖTELEZETTSÉGEI

Az elektronikus levelezésben is érvényesek az egyének közötti társalgás és levélírás alapvető illemszabályai. Az elektronikus levelezésben be kell tartani a levelezési konvenciókat.

A felhasználók elektronikus levelezéssel kapcsolatos jogai, kötelezettségei, illetve a használattal kapcsolatos szabályok megegyeznek az 5.8.1.2 Az Internet használatával kapcsolatos szabályok, biztonsági előírások fejezetben foglaltakkal, ezen felül az elektronikus levelezőrendszer felhasználóira a következő további szabályok vonatkoznak:

- a levél nem tartalmazhat olyan adatot, amely ***Biztonsági Osztályba Sorolási eljárásrend*** (***1. számú melléklet***) szerint 3. vagy ettől magasabb bizalmassági kategóriába került besorolásra;
- a csatolt fájloknak vírusmentesnek kell lennie;
- a munkavégzéssel kapcsolatosan már nem használható leveleket rendszeresen el kell távolítani a felhasználók postafiókjából;
- a levelek és csatolt mellékletek együttes maximális mérete 10 MB lehet;

- a tárterületek védelmének érdekében a Hivatal informatikai rendszerén belül minimalizálni kell a fájlok küldését. Szükség esetén a fájl hozzáférhető módon történő elhelyezése után, a fájlra mutató linket kell elküldeni az elektronikus levélben. Általános szabály, hogy törekedni kell arra, hogy egy fájl, csak egy példányban legyen tárolva a rendszerben;
- az elektronikus postaládát minden felhasználónak lehetőség szerint munkanap - betegség, szabadság, tartós távollét esetét kivéve - legalább egyszer meg kell néznie;
- az elektronikus levél fejlécében található tárgy mezőt minden esetben kötelező kitölteni;
- a levelek végén a Hivatalnál használt szabványos aláírást fel kell tüntetni;
- tilos a magáncélú levelek Hivatali emailcímre történő továbbítása;
- tilos a Hivatal által biztosított emailcímről magáncélú levelek küldése;
- tilos a Hivatal által biztosított emailcímről a levelek továbbítása magán emailcímre. (pl: átirányítás);
- a címzett mezőben maximum 5 címzett szerepelhet;
- tilos lánclevelek/gerillamarketing tartamú levelek indítása, vagy továbbítása.

A felhasználóknak tilos a Hivatal nevében olyan e-mailt küldeni, amelyek:

- a Hivatal hírnevét, vagy az ügyfelekkel való kapcsolatát ronthatják, illetve ügyfeleinek érdekét sérthetik,
- sérthetik mások becsületét, személyiségi jogait, etnikai, nemzetiségi hovatartozását, vallási, politikai meggyőződését
- törvényt, illetve a belső szabályait sértik,
- szerzői jogokat sérthetnek,
- vírusokkal fertőzhetnek meg bármely hálózatot.

Az elektronikus levélhez csatolt mellékleteket Hivatal standard szoftverekkel kell előállítani, hogy a címzett is el tudja olvasni azokat. Ha ez valamely okból nem tartható be, akkor a mellékletet tartalmazó levélben ezt jelezni kell, illetve a küldése előtt meg kell egyezni a címzettel a szoftvert, verziót és formátumot illetően.

Amennyiben a felhasználó szabadságra megy, betegszabadságon van, köteles a postafiókjában az „Automatikus válaszok (Házon kívül)" elnevezésű funkciót aktiválni – mind a szervezeten belüli, mind a szervezeten kívüli levélforgalom vonatkozásában – és abban megjelölni a távolmaradásának időtartamát, továbbá a helyettesítésére kijelölt személy nevét és annak elérhetőségét.

A felhasználóknak rendszeres ellenőrzés és archiválás útján gondoskodniuk kell arról, hogy a személyes postafiókjuk mérete ne lépje túl az engedélyezett keretet.

Az elektronikus postafiókba érkező, ismeretlen feladótól (gyanús, értelmezhetetlen vagy idegen nyelven íródott) származó, nem szokványos formátumú, gyanús csatolmányt tartalmazó, illetve idegen nyelvű küldeményekkel - a fennálló vírusveszély miatt - fokozott óvatossággal kell eljárni. Gyanús küldemény érkezésekor, illetve a vírusvédelmi rendszer riasztása esetén haladéktalanul értesíteni kell az informatikust. A csatolmányt ilyen esetben megnyitni nem szabad.

Nagyméretű (25 MB-nál nagyobb) állományt a Hivatalnál standard tömörítő (.zip) program segítségével tömörített formában kell elküldeni. Ha a mellékletek tömörített mérete meghaladja a maximálisan küldhető méretet, akkor több levélben kell a küldést elvégezni.

Amennyiben lehetséges a fájlok megküldésére a Hivatalnál az erre a célra alkalmazott szolgáltatást (ftp, sftp, hivatali kapu, cégkapu, e-papír) kell igénybe venni.

A levelező rendszerben található adatok hitelességét egyéni felhasználónévvel és jelszóval kell védeni.

A következő kiterjesztésű állományok elektronikus úton, mellékletként történő továbbítása nem engedélyezett a Hivatal informatikai rendszerében: bas, bat, cmd, com, cpe, inf, msp, msg, mst, reg, scr, vbs, exe stb. Az informatikus a felsorolt állományok küldését megakadályozó technikai jellegű intézkedéseket hajthat végre, illetve módosíthatja a kiterjesztések listáját.

5.9. ADATOK KEZELÉSE, TÁROLÁSA

A fájlmegosztások könyvtárszerkezetét, felépítését a jegyző, az adatgazdák és az informatikus közösen határozzák meg. A hozzáférési jogosultságok rendszerét úgy kell kialakítani, figyelembe véve a szakterület igényeit, hogy az informatikai biztonság követelményei megvalósuljanak.

Az adatok megőrzése, tárolása során be kell tartani az ágazati és adatvédelmi jogszabályokban, valamint a belső, adatkezelésekre vonatkozó szabályzatok (pl iratkezelési szabályzat, adatvédelmi szabályzat, stb.) előírásait.

A fájlmegosztásokat úgy kell kialakítani, hogy azok tartalmához csak a jogosultsággal rendelkező felhasználók férjenek hozzá, jogosultságaiknak megfelelően. A Hivatal munkatársai az általuk kezelt fájlokat a munkafolyamat befejezése után kötelesek a Hivatal alkalmazásaiba, vagy központi fájl tárolóeszközére feltölteni.

A Hivatal számítógépeiről, szervereiről - a munkahelyi célú felhasználás kivételével - szigorúan tilos programok, a 2. vagy ettől magasabb bizalmassági kategóriába sorolt adatot tartalmazó adatállományok, illetve a munkavégzés során szerzett egyéb adatok, információk magáncélú másolása, azok más, illetéktelen személyekkel történő megismertetése.

A munkaállomásokon a felhasználóknak tilos hálózati szolgáltatásként mappákat/fájlokat megosztani. (Windows Share szolgáltatás)

Adatok megosztása az alábbiak szerint lehetséges:

- munkatársak között a fájlszerverre, fájltárhelyre való felmásolással oszthatók meg adatok,
- külsős partnerek, harmadik felek részére, illetve szükség esetén munkatársak között is, a Hivatal által biztosított privát felhős fájlmegosztási szolgáltatást lehet használni a következő feltételekkel:
    - jelszóval le kell védeni a megosztási linken keresztüli hozzáférést,
    - be kell állítani a megosztási link érvényességi idejét, a megadott időpont után a linknek automatikusan meg kell szűnnie, elérhetetlenné kell válnia.

Hálózatra csatlakoztatott gépen a hivatalos dokumentumokat a hálózaton erre a célra kijelölt mappában kell tárolni, mert így biztosított a rendszeres és ellenőrzött mentés.

A Hivatal informatikai eszközein csak a munkavégzéshez szükséges adatokat szabad tárolni. A Hivatal informatikai eszközein TILOS tárolni:

- magán dokumentumokat,
- nem a munkavégzéshez szükséges képeket, filmeket,
- illegálisan letöltött jogvédett fájlokat, tartalmakat (multimédiás tartalom, szoftver, dokumentum),
- szoftverek védelmi rendszerének, integritásának megsértését előidéző alkalmazásokat (crack programok, kulcsgenerátorok),

- illegális licence kulcsokat,
- nem a munkavégzéshez szükséges programok, program telepítőkészleteket.

Az informatikus köteles a Hivatal központi fájltároló eszközeit rendszeresen 6 havonta átnézni, és nem engedélyezett tartalom esetén eljárni az alábbiak szerint:

- megállapítani a tiltott tartalom feltöltőjének tulajdonosát,
- jegyzőkönyvet felvenni az incidensről,
- törölni a nem engedélyezett tartalmat.

Az adatvédelmi incidensről készített jegyzőkönyvet az informatikusnak alá kell írnia és el kell juttatni a jegyzőhöz aki a szükséges intézkedést elrendeli.

A felhasználók számítógépein az ellenőrzéseket évente legalább 1 alkalommal el kell végezni. Ha a számítógépen nem engedélyezett tartalom található, ugyanúgy kell eljárni, mint a központi fájltároló eszköz esetében.

A felhasználók felelősek a munkaállomásaikon (sajátgép) tárolt és a szerverre fel nem töltött adatok megsemmisüléséből keletkezett károkért.

Automatizált törlési megoldással biztosítani kell:

- számítógépek, laptopok esetén az ideiglenes fájlok, valamint a törlésre kijelölt fájlok (pl: Lomtár tartalma, rendszer temp könyvtárai, internet böngészők temp könyvtárai) hetente történő törlését,
- a közös használatú, ideiglenes tárolásra használt mappák napi szintű törlését (pl: közös, scannelt anyagokat tartalmazó mappa).

A felhasználónak kötelessége a számítógépén és a hálózati meghajtón, a központi tárterületen található személyes mappájában tárolt, általa készített vagy kezelt dokumentumainak rendszeres szinkronizálása. Azokat az állományokat, melyek nem szükségesek, törölni kell a rendszerből. A törlési feladatot teljes felelősség vállalása mellett a munkavállaló végzi.

A központi szerver tárkapacitásának túlterheltsége esetén, a központi tárterületeken tárolt adatok rendszeres (féléves, éves) karbantartása érdekében az adatgazdák együttműködve az informatikussal elvégzik a felesleges adatok, illetve a megfelelő mentési és archiválási eljárás során lementett adatok törlését.

Az adatgazdáknak vagy felettes vezetőknek évente át kell nézniük a fájlmegosztásokat és a jogalap nélkül tárolt dokumentumokat le kell törölniük az iratkezelési szabályzatnak megfelelően. A postafiókokban csak jogalappal tárolhatók adatok, dokumentumok, erről a felhasználóknak kell gondoskodniuk.

Évente legalább egy alkalommal ellenőrizni kell a Hivatal által használt fájlmegosztások tartalmát, és a jogosulatlanul megosztott vagy szerzői joggal védett anyagok elérését meg kell szüntetni.

A több osztály által használt vagy alap biztonsági zónában található több funkciós nyomtatókat az informatikusnak úgy kell konfigurálnia, hogy a nyomtatás csak a felhasználó saját PIN kódjának beírása után kezdődjön el.

Amennyiben a nyomtató rendelkezik saját merevlemezzel, akkor havonta 1 alkalommal ellenőrizni kell, és tartalmukat le kell törölni, vagy a belső adattároló eszközt ki kell szerelni a nyomtatóból.

5.10. ADATHORDOZÓK KEZELÉSE

Jelen fejezet alapján kerülnek rögzítésre az informatikai adathordozók használatba vételével, tárolásával, használatból kikerülésével, illetve selejtezésével kapcsolatos biztonsági követelmények.

5.10.1. HASZNÁLATBA VÉTEL, JELÖLÉS

Nyilvántartást kell vezetni a munkatársaknak kiadott adathordozók típusáról, és adatairól.

Minden adathordozót újraalkalmazása előtt az adatok megsemmisítését eredményező megfelelő eljárással törölni kell.

5.10.2. TÁROLÁS

A tároláshoz szükséges káros hatások (túl magas hőmérséklet, por, nedvesség, páratartalom, elektromágneses behatások) elleni védelmet biztosító tárolóeszköz használata. A tároláskor figyelembe kell venni az adattároló eszköz gyártói által specifikált környezetet, amely mellett az eszköz a leghosszabb ideig képes az adatokat megőrizni.

A tartalék vagy ideiglenesen nem használt adathordozók tárolóhelye csak az informatikus számára legyen hozzáférhető.

5.10.3. AZ ADATHORDOZÓK HASZNÁLATÁNAK, SZÁLLÍTÁSÁNAK FELTÉTELEI, KÖVETELMÉNYEI

Idegen, talált pendrive-ot a Hivatal tulajdonában levő számítógépre csatlakoztatni TILOS! A mások által véletlenül vagy szándékosan elhagyott pendrive-ok vírust tartalmazhatnak.

Ezen rendelkezések az adatok és az adatokat fizikailag tároló adathordozók kezelésére vonatkoznak.

Az adathordozók biztonságos tárolása és szállítása érdekében az alábbi szempontokat kell figyelembe venni:

- az adathordozókat óvni kell a fizikai sérülésektől;
- az adathordozók állapotát rendszeresen ellenőrizni kell. A saját használatra kiadott adathordozó eszközök állapotának ellenőrzése a felhasználók feladata. Azt az adathordozót, melyet fizikai károsodás ért, vagy a megengedett hibahatárt elérte, selejtezni kell;
- Szállítási céllal történő mozgatás esetén a nem nyilvános adatot tartalmazó adathordozón lévő adattartalmat másolni szigorúan tilos!
- A 2. vagy ettől magasabb bizalmassági kategóriába sorolt adatot adathordozón csak titkosítva szabad tárolni.

A Hivatal számítógépeihez csak a Hivatal által biztosított adathordozókat szabad csatlakoztatni. Az adathordozók csatlakoztathatóságát a jegyző utasítására az informatikus korlátozhatja hardver vagy szoftver eszközzel.

A Hivatal informatikai rendszerébe kapcsolt munkaállomásokon csak olyan adathordozót lehet használni, arról adatokat beolvasni, amelyen előtte a rendszeresített és telepített víruskereső programmal vírusellenőrzést végeztek.

A Hivatal által biztosított adathordozón magánjellegű adatot tárolni tilos.

A mobil infokommunikációs eszközök, mobil adathordozók felhasználói felelősek az eszközön található adatok esetleges kiszivárgásáért, az eszköz elvesztéséért, eltűnéséért, megsérüléséért.

5.10.4. ADATHORDOZÓK TÖRLÉSE

Az informatikai berendezéseken tárolt információk kikerülése akkor is veszélyeztetheti a Hivatal érdekeit, ha egy bizonyos eszközt (például merevlemezt, mágnesszalagot, stb.) ideiglenesen, vagy véglegesen kivonnak a használatból. Ezért ezekről az eszközökről az eszközök tárolásra való felkészítésekor, a szervezet ellenőrzési körén kívülre kerülés előtt, az adatokat az informatikusnak véglegesen, visszaállíthatatlanul törölnie kell.

Az adathordozók törléséhez szükséges szoftver licencnek mindig a legfrissebb verzióját kell alkalmazni.

5.10.5. ADATHORDOZÓK SELEJTEZÉSE

Az adathordozók selejtezésére vonatkozó előírásokat az Informatikai ***Selejtezési szabályzat (2. számú melléklet)*** tartalmazza.

5.10.6. A HIVATAL HATÁSKÖRÉBŐL KIKERÜLŐ ADATHORDOZÓK

A nem nyilvános adatot tartalmazó hordozható adathordozók (mobil merevlemez, pendrive) adataihoz az informatikusnak felhasználót kell nevesítenie, aki felelős az adott hordozó adatainak biztonságáért.

Az informatikai rendszerek offline adatszolgáltatásához (hagyományos postai, illetve futár általi szállítás) használatba vett adathordozót nyilvántartásba kell venni, és dokumentálni szükséges az adatátadást. (pl: Iktatás)

5.11. RENDSZEREK FELÜGYELETE

A rendszerek naplózására vonatkozó szabályozást, valamint a naplózási beállításokat rendszeresen, évente legalább egyszer felül kell vizsgálni.

Az informatikai eszközök monitoring és naplózó rendszerének alkalmasnak kell lennie egy esetleges hacker támadás jelzésére, a megadott figyelési paraméterek szerint.

Az informatikai rendszerek által biztosított naplóadatokból meg kell tudni állapítani a rendszer jogosulatlan használatát.

Az informatikai rendszerek biztonsági és használati naplózásának beállítását egyeztetni kell azon szervezeti egységekkel, melyek az elkészült naplók feldolgozását, riportolását végzik, vagy munkájuk során bármilyen formában feldolgozzák a naplók tartalmát.

Az informatikai rendszer működését és biztonsági állapotát az informatikai rendszer működési ideje alatt folyamatosan felügyelni kell. Ennek keretében monitorozni kell, ha az értelmezhető az informatikai rendszerre:

- hardver erőforrások kihasználtságát,
- hőmérséklet értékeket,
- futó folyamatok, szolgáltatások elérhetőségét,
- sikertelen bejelentkezési kísérletek,

- adminisztrátor jogú felhasználók sikeres bejelentkezését,
- hálózati kapcsolaton zajló folyamatok (nyitott kapcsolatok, sikertelen kapcsolódási kísérletek, stb.)

Az informatikai rendszer ellenőrizendő paramétereit, valamint az ellenőrzések ciklus idejét egyedileg kell meghatározni. Az informatikai rendszert érintő változás esetén (pl: szoftver változás, elérhetőség változás, stb.), felül kell vizsgálni az ellenőrizendő paraméterek szükségességét, ciklus idejét és aktualizálni kell az új felteleknek megfelelően.

Az eszközfelügyeleti rendszereket, naplózó rendszert úgy kell konfigurálni, hogy a riasztási küszöb elérése esetén az informatikus email értesítést kapjon. A normál működés maximum értékeit kell riasztási küszöbértéknek venni. Az esetleges hibákról a felügyeleti rendszernek riasztást kell küldenie, legalább a kritikus fontosságú eszközök esetében. A felügyeleti rendszer által küldött riasztásokat az informatikusnak ki kell vizsgálnia.

A felügyeleti rendszernek a hardver eszközöket, szoftver és firmware verziók aktuális állapotát naplóznia kell.

Amennyiben az informatikai rendszer felügyeletével, naplózásával kapcsolatban jogi aggályok merülnek fel, úgy szakhatóságtól vagy szakjogásztól állásfoglalást kell kérni. Az informatikai rendszer felügyeletének, naplózásának kialakításakor figyelembe kell venni a jogi állásfoglalást.

5.11.1. RENDSZER ESEMÉNYEK NAPLÓZÁSA

Az informatikai (al)rendszereknek automatikusan tárolnia kell a folyamatokhoz tartozó meghatározott biztonsági adatokat (a szükséges mértékben) a hatékony biztonságkezelés érdekében.

A naplóadatok tárolására megfelelő méretű, és felülírástól védett munkaterületet kell biztosítani a háttértároló rendszeren.

A nyomkövetési (napló)adatokat áttekinthető szerkezetben kell tárolni, és adott esetben rendelkezésre kell bocsátani a feljogosítottak számára.

A központi naplóelemző rendszerben kell gyűjteni minden kritikus informatikai rendszerelem (tűzfal, router, switch, szerver, kritikus adatkezelő alkalmazás) naplóit és a rendszernek az előre beállított feltételek szerint folyamatosan elemezni kell a naplók tartalmát.

5.11.1.1. NAPLÓZÁS HATÁLYA

Az informatikai rendszerekben történt konfiguráció-módosítást, beállítások megváltoztatását, valamint rendszerelemek üzembeállítását, illetve üzemből történő kivonását rögzíteni kell.

A naplófájlnak tartalmaznia kell legalább a következőket:

- a felhasználó azonosítóját,
- a naplóbejegyzés idejét,
- a naplózott eseményt,
- a napló sorszáma.

Naplózni kell az alábbi eseményeket:

- a be- és kijelentkezés dátumát és időpontját,
- a sikeres és a sikertelen rendszer-hozzáférési kísérletekről készült feljegyzéseket (rekordokat),

- a sikeres és a sikertelen adathozzáférési és más erőforrás-elérési kísérletekről készült bejegyzéseket,
- jogosultság változások,
- beállítások változása,
- felhasználói hozzáférések létrehozása, engedélyezése, letiltása, törlése,
- amennyiben az információ releváns, az alábbi információkat is tartalmazzák a naplóbejegyzések:
    - a munkaállomás azonosítója,
    - szoftverek konfigurációjában végzett változások,
    - tűzfalon zajló változások, távoli bejelentkezések monitorozása,
    - hardver hibák naplóbejegyzései,
    - fájlműveletek,
    - adatbázis műveletek.

Az események naplózása során törekedni kell, csak a legszükségesebb események naplózására. A naplózandó események meghatározásakor figyelembe kell venni az informatikai biztonsági felelős, valamint az adatgazdák javaslatait. Egy bekövetkezett incidens javítása után, amennyiben szükséges szigorítani kell a naplózási beállításokat, kiemelt figyelmet kell fordítani az érintett informatikai rendszerre. Hatósági, vagy felettes szerv által kiadott riasztás alapján, ha szükséges új naplóelemzési és riasztási szabályokat kell létrehozni.

A naplókezelő rendszer beállításait, a naplózásra és riasztásra kijelölt eseményeket a naplókezelő rendszer vagy az elektronikus információs rendszer vagy annak környezetében bekövetkezett változáskor, de legalább évente egy alkalommal felül kell vizsgálni.

Incidens bekövetkezésekor, vagy egy incidens bekövetkezési kockázatának növekedésekor a riasztási küszöbértékeket felül kell vizsgálni, esetleg újabb felételeket kell bevonni a naplóelemzésbe. A szükséges módostásokra az informatikai biztonsági felelős tesz javaslatot.

A naplóbejegyzéseket szabványos, a naplókezelő és/vagy a naplóelemző rendszer által feldolgozható formátumban kell előállítani és tárolni.

5.11.1.2. NAPLÓK VÉDELME

A naplóeszközöket a jogosulatlan hozzáférés ellen védeni kell.

A nyomkövetési napló adatait védeni kell az illetéktelen megismerés, (véletlen vagy szándékos) módosítás és megsemmisítés ellen a biztonsági fokozatnak megfelelően.

A naplóállományokat - amennyiben az eszköz/szoftver erre alkalmas - minimum 30 napig meg kell őrizni, az ehhez szükséges tárterületről az informatikusnak kell gondoskodnia. A biztonsági napló állományok és minden kapcsolódó dokumentum (riportok, jelentések) titokköri besorolása megegyezik az adott rendszer által kezelt adatok besorolási szintjével.

A központi naplóelemző rendszer tárhelykapacitását úgy kell méretezni, hogy legalább 30 napra visszamenőleg megőrizze a naplóállományokat. A központi naplóelemző rendszernek haladéktalanul riasztást kell küldenie az informatikusnak, ha a tárhely foglaltsága eléri a 80%-ot.

A központi naplóelemző rendszerben tárolt naplóállományokhoz az informatikus csak olvasási jogosultsággal férhet hozzá és a naplókat titkosítással védeni kell a közvetlen hozzáférés megakadályozása érdekében.

5.11.1.3. HIBÁK NAPLÓZÁSA

A felhasználók és rendszerprogramok által jelentett hibákat naplózni és elemezni kell, ezek alapján meg kell tenni a megfelelő intézkedéseket.

5.11.1.4. NAPLÓK ELEMZÉSE, RIASZTÁS

Az informatikus felelőssége és feladata, hogy a naplóállományok rendszeresen átvizsgálásra kerüljenek. Az elemző szoftvert úgy kell konfigurálni, hogy automatikusan, haladéktalanul riasztást küldjön az informatikusnak és az informatikai biztonsági felelősnek, ha a biztonság megsértésére vagy az eszköz nem megfelelő működésére utaló naplóbejegyzést észlel.

A naplózó rendszer leállása, a naplófájlok elérhetetlensége esetén a rendszernek riasztást kell küldenie jegyzőnek és az informatikai biztonsági felelősnek.

Amennyiben a naplófájlok az információ biztonság megsértésére, vagy annak kísérletére irányuló bejegyzést tartalmaznak, úgy ki kell vizsgálni a lehetséges támadást, a ***Biztonsági Eseménykezelési eljárásrendben*** megfogalmazottak szerint.

Legalább a szerverek esetén, ha a sikertelen bejelentkezési kísérletek száma meghaladja a 24 óra alatt a 100 db-ot, a felügyeleti rendszernek riasztást kell küldenie.

A felettes hatóságtól, eseménykezelő központtól kapott vagy hazai, nemzetközi riasztások alapján, a naplók elemzését felül kell vizsgálni, szükség esetén a riasztásokat újra kell konfigurálni, vagy kiegészítő riasztásokat kell beállítani, az esetleges támadások időben történő észlelésére.

A naplóelemző és az informatikai felügyeleti rendszer által készített jelentéseket az informatikai biztonsági felelős havonta megvizsgálja és negyed évente írásos összegző jelentést készít a jegyzőnek, az eseményekről és a biztonsági állapotról.

5.11.2. RENDSZEREK ÓRÁJÁNAK SZINKORNIZÁLÁSA

Az informatikai eszközök óráit azonos értékre kell beállítani így szavatolható az eseménynaplók pontossága, amelyek adott esetben vizsgálatokhoz is szükségesek lehetnek.

Ahol a szerver vagy hálózati eszköz valós, hálózati időszolgáltatást tud nyújtani az informatikai infrastruktúra számára, akkor azt ajánlatos egy nemzetközi órajelszolgáltatóhoz szinkronizálni és a helyi informatikai eszközöket ehhez a központi hálózati időszolgáltatáshoz konfigurálni.

Az informatikai eszközök pontos dátumának és órájának beállítására olyan eljárást kell alkalmazni, amely az időeltérést ellenőrzi és kijavítja.

6. HOZZÁFÉRÉSEK KEZELÉSE

A hozzáférések kezelése szervezet szintű, az egyes szervezeti egységek vezetői határozzák meg munkatársak jogosultságait.

A Hivatal informatikai rendszereiben kezelt adatokhoz és működtető programokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - amelynek megvalósítása különböző (pl. felhasználói név és jelszó) – lehet hozzáférni.

Az azonosítás és a hitelesítés folyamatainak meg kell előznie az információs rendszerrel kapcsolatos bármilyen más engedélyezett beavatkozást.

A kliens-szerver alkalmazásoknál az azonosításnak és a hitelesítésnek mind a kliens, mind a szerver oldalon meg kell történnie, amelynek erőssége különböző lehet.

A felhasználói azonosítást egyértelműen kell hozzárendelni minden egyes személyhez, azaz kerülni kell, hogy több személy azonos, közös hozzáférési azonosítót használjon. Amennyiben a csoportos felhasználói azonosító használata elkerülhetetlen (pl: központi rendszerek esetén), úgy bármely a hozzáférést használó munkatárs távozása esetén, az adatgazdának azonnal meg kell változtatnia a hozzáférés jelszavát.

A hozzáférési jogosultságok tekintetében a szükséges minimális jogok odaítélésére kell törekedni.

A hibás vagy sikertelen bejelentkezési kísérletekre megfelelő óvó- és ellen intézkedésekkel kell reagálni.

Az informatikai rendszer minden meghatározó eleme rendelkezzen olyan védelmi mechanizmusokkal, amely megakadályozza illetéktelen személyek logikai hozzáférését a védett rendszerhez. Ellenőrizni kell, hogy a felhasználónak van-e engedélye az informatikai rendszer, vagy alkalmazás használatára.

Az adatkezelési biztonsági rendszer moduláris legyen így biztosítsa, hogy különféle hozzáférési kritériumok alapján meg lehessen határozni, az adatbázisok tartalmához, dokumentumokhoz, szolgáltatásokhoz történő hozzáférés jogosultsági szintjeit (írás, olvasás, törlés, stb.).

6.1. FELHASZNÁLÓ AZONOSÍTÓK HASZNÁLATA, MŰKÖDÉSE

Az alapértelmezett hitelesítési adatokat (felhasználónév-jelszó) meg kell változtatni, a Hivatal hozzáférésekre vonatkozó szabályainak megfelelően.

Hitelesítéshez használt tanúsítványokat, hitelesítő eszközöket (hardver vagy szoftver token) egyértelműen kell hozzárendelni minden egyes személyhez, nem használhat több személy azonos, közös hitelesítő eszközt.

A felhasználók a következő egyedi biometrikus tulajdonságaik alapján is hitelesíthetik magukat operációs rendszer szinten: ujjlenyomat, retina. Ha a hitelesítés 3 alkalommal sikertelen a rendszernek jelszót kell kérnie. A sikertelen bejelentkezési kísérletről naplóbejegyzést kell készítenie rendszernek.

A számítógépes felhasználói azonosítók létrehozásának célja, hogy lehetővé tegye az adatok és az erőforrások használatát a felhasználó számára, úgy, hogy az a munkaköri feladatainak ellátásához szükséges mértékű legyen. A jogosultságok beállításakor minden erőforrás esetén (fájltárhely, nyomtató, stb.) a szükséges minimum elvét kell alkalmazni.

Az informatikai rendszerek (könyvtárak, adatbázisok, nyomtatók) jogosultsági szintjeinek kialakítása érdekében a lehetséges tevékenységek, és munkakörök figyelembevételével felhasználói csoportokat

kell definiálni és egy-egy felhasználói azonosító meghatározásakor a csoportba vagy csoportokba sorolást el kell végezni.

A rendszerhez és szolgáltatáshoz történő hozzáférési jogot csak szabályszerű nyilvántartásba vételi eljárást követően lehet megadni.

Az informatikai eszközöket, valamint a hálózathoz való hozzáférést névre szóló felhasználói azonosítóval (felhasználói név + jelszó) kell védeni.

A Hivatalhoz nem tartozó személyek számára felhasználói azonosítót kizárólag az adatgazda írásos engedélyével szabad létrehozni.

Amennyiben az adott informatikai rendszerelemben beállítható, úgy alkalmazni kell a következő szabályokat:

- a felhasználói hozzáférést automatikusan le kell tiltani 5 sikertelen belépési kísérlet után 30 percre. A felhasználó az informatikusnál kezdeményezheti letiltott felhasználói hozzáférésnek engedélyezését.
- ha egy felhasználói azonosító (technikai és felhasználói hozzáférése esetén egyaránt) 60 napig inaktív, akkor informatikusnak kézzel kell letiltania a hozzáférést, úgy hogy a felhasználói azonosító tulajdonosának az informatikushoz kelljen fordulnia a felhasználói azonosító újbóli aktiválása érdekében. Letiltott felhasználói hozzáférés engedélyezésének folyamata megegyezik a 6.1.2 Felhasználói jogosultságok megszüntetése, megváltoztatása fejezetben leírtakkal.
- Első belépéskor a felhasználót tájékoztatni kell a képernyőn megjelenő üzenetben, hogy az általa végzett tevékenységet naplózza a rendszer és az általa használt felhasználói hozzáférés nevében végzett valamennyi műveletért felelősséggel tartozik. „Ön a Kenderes Polgármesteri Hivatal rendszerét használja, a rendszer használatát figyelhetik, rögzíthetik, naplózhatják, a rendszer jogosulatlan használata tilos és büntetőjogi vagy polgárjogi felelősségre vonással jár, a bejelentkezéssel fentieket tudomásul veszi"
- az 1 évnél hosszabb ideig letiltott felhasználói hozzáférést meg kell szüntetni, ha a jegyző másképp nem rendelkezik, a felhasználó profiljához rendelt adatokat automatizáltan le kell törölni, vagy a felettes vezető által meghatározottak szerint meg kell őrizni,
- letiltott, vagy helyreállítást igénylő felhasználói fiók esetén, a helyreállítás során az az informatikus egy ideiglenes jelszót rendel a felhasználói azonosítóhoz és ki kell kényszeríteni a jelszó cserét,
- a rendszer ne mutassa az utoljára bejelentkezett felhasználó nevét,
- a vendég, illetve jelszó nélküli felhasználói hozzáféréseket le kell tiltani,
- egyszeri bejelentkezési képességet (SSO) kell kialakítani, a jogosultságok egyszerűbb, központi kezelése és a hitelesítő adatok csökkentése érdekében,
- A kezdeti vagy ideiglenes jelszavak generálása esetén is be kell tartani a jelszavak bonyolultságára vonatkozó kötelező előírásokat. A rendszer lehetőség szerint a felhasználót kényszerítse a felhasználói azonosító első használatakor a (informatikus által neki kijelölt) jelszavának megváltoztatására. Ennek minden olyan esetben is be kell következnie, amikor az informatikus egy ideiglenes jelszót rendel a felhasználói azonosítóhoz.
- Mind a sikeres, mind a sikertelen belépési és kilépési kísérleteket naplózni kell.
- a hitelesítés során olyan technológiát, beállításokat kell alkalmazni, amely véd a hitelesítő adatok visszajátszásától, a felhasználó megszemélyesítésétől,

A felhasználónév a következő névkonvenció alapján kerül meghatározásra, amennyiben az adott rendszerben megvalósítható:

- vezetéknév.keresztnév (központi címtár esetén)
- vezetéknév.keresztnév (lokális hozzáférés esetén)

Adatkezelő alkalmazások vagy szolgálatások esetén felhasználónév a következő névkonvenció alapján kerül meghatározásra, amennyiben az adott rendszerben megvalósítható: VezetéknévKeresztnév vagy email cím.

A felhasználói azonosítók kezelésre vonatkozó általános előírások:

- A felhasználói hozzáféréshez tartozó felhasználónevet az informatikus, az adatgazda, illetve a harmadik fél személyesen adja át vagy emailben küldheti meg a felhasználó részére. A belépéshez szükséges jelszót személyesen vagy SMS-ben küldheti meg a felhasználó részére. A felhasználónevet és a jelszót tilos ugyanazon elektronikus kommunikációs csatornán keresztül megküldeni.
- Kéttényezős hitelesítés esetén a felhasználónak kell beállítania a hitelesítő eszközt az informatikus, az adatgazda, vagy a szolgálató útmutatása alapján. Hardverkulcs esetén jegyzőkönyvezni kell az átadást.
- A felhasználói azonosító tulajdonosa felelős a felhasználói azonosítója nevében végzett valamennyi tevékenységért, a szervezet által birtokolt adatok és erőforrások védelméért, etikus módon történő használatáért.
- A felhasználói azonosítókkal kapcsolatos minden incidenst (téves bejelentkezés vagy elöregedés miatti kitiltás, a jelszónak nem a tulajdonos által történő megváltoztatása stb.) jegyzőkönyvezni kell, és a jegyzőnek írásban jelenteni.
- Egy letiltott felhasználói azonosító ismételt felhasználása nem lehetséges a letiltást követő 60 napig.
- A munkaviszonyukat huzamosabb ideig szüneteltető, vagy a munkavégzésben hosszabb ideig más ok miatt részt nem vevő felhasználók azonosítóját újra munkába állásukig fel kell függeszteni (inaktiválni kell). Az azonosító újraaktiválási igényének felmerülésekor a hozzáférés helyreállítását szintén a közvetlen felettes kérheti.

Olyan védelmi rendszert kell alkalmazni, amely a hitelesítési eljárás során kizárja a bejelentkezést, ha egy előírt jelszó-érvényességi időtartamon belül a bejelentkező nem változtatta meg a jelszavát. Ezt a védelmi funkciót engedélyezni kell a rendszerek beállítása során.

6.1.1. FELHASZNÁLÓI JOGOSULTSÁGOK LÉTREHOZÁSA

Új munkatárs belépésekor, vagy ha egy munkatárs új munkakörbe kerül, vagy a munkakörhöz tartozó feladatokkal kapcsolatban ez szükségessé válik, munkatárs felettes vezetője megigényli a munkatárs felhasználói azonosítójának/azonosítóinak, valamint a leendő munkahelyi környezetének létrehozását. Ehhez kitölti a ***Felhasználói jogosultság igénylő lap (8. számú melléklet)*** és ***Munkahelyi környezet létrehozása/megszüntetése (7. számú melléklet)*** formanyomtatványokat a munkatárs számára a munkaköri feladatainak az ellátásához. Az igénylést az adatgazda véleményezi. Az adatgazda vagy az informatikus feladata a csoportba sorolás és a csoport jogosultságon felüli jogok meghatározása.

Harmadik fél részére felhasználói hozzáférést, csak a jegyző által kitöltött ***Felhasználói jogosultság igénylő lap (8. számú melléklet)*** alapján szabad létrehozni.

Az informatikus vagy adatgazda a kitöltött és a jegyző által jóváhagyott igénylőlap alapján létrehozza a rendszerekben az igényelt azonosítókat, kialakítja a munkahelyi környezetet, amit aláírásával igazol, és frissíti a jogosultság nyilvántartást. ***(3. számú melléklet –Jogosultság kiosztási nyilvántartás)***

A ***Felhasználói jogosultság igénylő lap (8. számú melléklet)*** és ***Munkahelyi környezet létrehozása/megszüntetése (7. számú melléklet)*** igénylőlapokat az informatikus tárolni köteles.

6.1.2. FELHASZNÁLÓI JOGOSULTSÁGOK MEGSZÜNTETÉSE, MEGVÁLTOZTATÁSA

Ha egy munkatárs valamely vagy összes munkaköre megszűnik (áthelyezés, felmondás stb. során), a felhasználói azonosítóit, valamint a munkahelyi környezethez kapcsolódó hálózati hozzáféréseket haladéktalanul le kell tiltani, majd amennyiben lehetséges, meg kell szüntetni. A munkatárs felettes vezetője megigényli a munkatárs felhasználói azonosítójának/azonosítóinak, valamint a munkahelyi környezetének megszüntetését, módosítását. Ehhez kitölti a ***Felhasználói jogosultság igénylő lap (8. számú melléklet)*** és ***Munkahelyi környezet létrehozása/megszüntetése (7. számú melléklet)*** című formanyomtatványokat. Az igénylést az adatgazda véleményezi, és továbbítja a jegyzőnek. A kitöltött igénylőlapok alapján az adatgazda vagy az informatikus megszünteti a megfelelő rendszerekben az igényelt azonosítókat, a munkahelyi környezetet, amelyet az aláírásával igazol.

A jegyző jogosult arra, hogy bármely munkatárs valamely vagy összes érvényben lévő felhasználói azonosítóját azonnali hatállyal letiltathassa. A szükséges adminisztrációt ebben az esetben is el kell végezni, azonban ebben az esetben elegendő utólag elvégezni a dokumentálást.

Harmadik fél részére felhasználói hozzáférést, csak a jegyző által kitöltött ***Felhasználói jogosultság igénylő lap (8. számú melléklet)*** alapján szabad módosítani, vagy törölni.

A kilépett munkavállaló felettes vezetője köteles rendelkezni a kilépett felhasználó levelezésének, adatainak, dokumentumainak további kezeléséről (archiválás, törlés, harmadik személy általi hozzáférhetőség).

Egy munkatárs jogviszonyának megszűnéséről a felettes vezetőjét, valamint a jogviszony megszűntetését végző adatgazdát vagy informatikus is értesíteni kell. A kilépő munkatárs munkaügyi papírjait csak a felhasználói azonosítóinak letiltása vagy törlése után szabad átadni.

6.1.3. JELSZÓMENEDZSMENT

A Hivatal kritikus rendszereiben használatos jelszavak tárolása és átvitele a hálózatokon (LAN és WAN) csak titkosítottan történhet, ezzel csökkentve a kockázatát, hogy a hálózati forgalom megfigyelésével valaki más felhasználó jelszavát megtudhassa, és más felhasználó nevében bejelentkezve jogosulatlan tevékenységeket végezzen.

A Hivatal informatikai rendszereihez való illetéktelen logikai hozzáférés megakadályozására jelszavas védelmet kell alkalmazni.

A Hivatal számítógépes hálózatába, illetve az alkalmazásokba bejelentkezési jogosultsággal rendelkező felhasználó köteles a bejelentkező nevéhez tartozó jelszó megőrzésére. A saját bejelentkező névhez tartozó jelszót mások által is elérhető módon feljegyezni nem szabad.

Azon informatikai rendszerek esetén, melyek rendelkeznek a megfelelő technikai feltételekkel, a hitelesítéshez használt **felhasználói** hozzáféréshez rendelt jelszavaknak az alábbi kritériumoknak kell megfelelni, az elvárásokat ki kell kényszeríteni:

- a felhasználói jelszavak minimális hossza 12 karakter;
- a felhasználói jelszavak minimum 1 napig legyenek érvényesek,

- a felhasználói jelszavak maximum 180 napig lehetnek érvényesek.,
- az utolsó 12 jelszót nem lehet újra használni,
- a jelszónak kisbetűt, nagybetűt és számot kell tartalmaznia, javasolt speciális karakterek használata is,
- a felhasználóknak meg kell változtatniuk a jelszavukat, amikor első alkalommal használják felhasználói azonosítójukat,
- ne tartalmazzon bármilyen nyelvű szót szótári alakban,
- ne egyezzen meg a felhasználó nevével, felhasználói azonosítójával, egyik telefonszámával sem, engedélyének számával, személyi számával vagy dolgozói kódjával, valamint a felhasználóhoz kötődő bármely karaktersorozattal (pl. születési dátum, lakcím),
- ne egyezzen meg személynévvel,
- ne egyezzen meg közéleti személyek nevével és egyéb közismert szavakkal, kifejezésekkel,
- ne tartalmazzon azonos, vagy ismert logika szerint egymást követő karaktereket (pl. 11111, aaaaa, qwert, asdfg, gegegeg),
- ne utaljon a felhasználóra, munkakörére, munkahelyére,

A fenti követelményekről minden felhasználót tájékoztatni kell munkájának megkezdése előtt.

Amennyiben indokolt és a Hivatal erőforrásai ezt lehetővé teszik, egységes jelszókezelő rendszert kell bevezetni. A jelszókezelő rendszer tegyen javaslatot biztonságos új jelszavak létrehozására.

Ha az informatikai rendszer arra alkalmas, akkor létre kell hozni egy jelszó listát, mely tartalmazza a rendszerben nem használható jelszavakat, az következők szerint: könnyen kitalálható jelszavak, kompromittált jelszavak. Célszerű a jelszó kezelő rendszer beépített jelszó ellenőrző funkciójának használata.

6.1.4. FELHASZNÁLÓK BEJELENTKEZÉSE

A Hivatal számítógépes hálózatába bejelentkezni csak a rendszerben definiált bejelentkező név és a hozzátartozó jelszó ismeretében lehet.

A több felhasználós informatikai rendszerek elérésénél a felhasználók megkülönböztetésére, illetve a bizalmasság és sértetlenség megőrzésére bejelentkezési eljárásokat kell definiálni.

A bejelentkezési eljárások meghatározásánál az alábbi biztonsági követelményeket kell figyelembe venni:

- egyéni felhasználói azonosítók használata, amely felhasználóhoz köthető és az ő műveleteiért felelős;
- ellenőrizni kell, hogy a felhasználónak van-e engedélye az informatikai rendszer, vagy alkalmazás használatára;
- a felhasználó a hozzáférési jogairól kapjon értesítést;
- listát kell készíteni az alkalmazásokat használó regisztrált személyekről;
- rendszeresen ellenőrizni kell, és el kell távolítani a felesleges felhasználói azonosítókat;
- biztosítani kell, hogy a feleslegessé vált felhasználói azonosítók ne kerüljenek ismét felhasználásra;

- az operációs rendszerhez, illetve az alkalmazói rendszerekhez való hozzáférés esetén, ahol lehet, az utolsó sikeresen bejelentkezett felhasználói azonosítónak rejtve kell maradnia.

6.1.5. HOZZÁFÉRÉSI JOGOSULTSÁGOK NYILVÁNTARTÁSA

A jogosultságokat a központilag kell nyilvántartani, névre szólóan kell meghatározni és beállítani.

A munkatársak által használt hitelesítő eszközökről nyilvántartást kell vezetni. (token, hardverkulcs). Az eszközök kompromittálódása, elvesztése, sérülése esetén a hozzárendelt jogosultságokat meg kell szüntetni, és cserélni kell az eszközt.

Az informatikus és az adatgazdák feladata a ***Jogosultság kiosztási nyilvántartást (3. számú melléklet)*** aktualizálása.

A nyilvántartásokat évente legalább egy alkalommal, illetve minden egyes releváns változást követően az informatikusnak felül kell vizsgálnia és ellenőriznie kell az aktuálisan beállított jogosultságokat. A felülvizsgálatot dokumentálni szükséges. Amennyiben eltérés állapítható meg a nyilvántartás és beállított jogosultságok között, és felmerül a gyanú, hogy visszaélés történt úgy incidensként kell kezelni az észrevételt.

A felülvizsgálat során ellenőrizni kell az összeférhetetlenségeket.

6.1.6. KIEMELT JOGOSULTSÁGOK KEZELÉSE

A kiemelt jogosultságok kiosztását és használatát (amely lehetővé teszi a rendszer vezérlésébe történő beavatkozást) korlátozni és ellenőrizni kell.

Az adminisztrátori szintű hozzáférés (operációs rendszerek, hálózati eszközök, alkalmazások, szolgáltatások) csak az informatikusok számára engedélyezett. Adatgazdák a hozzájuk rendelt, illetve kezelésükben lévő alkalmazások, szolgáltatások estén rendelkezhetnek adminisztrátor szintű jogosultsággal. Ettől eltérni csak a jegyző írásos engedélyével lehet.

Az adminisztrátori szintű hozzáférést csak a rendszerek karbantartásakor szabad használni, a napi munkavégzéshez az informatikusoknak is felhasználói jogosultsággal rendelkező hozzáféréssel kell használniuk.

Az adminisztrátori szintű hozzáféréseket (operációs rendszerek, hálózati eszközök) kétfaktoros hitelesítéssel kell védeni.

6.1.7. FELHASZNÁLÓI HOZZÁFÉRÉSEK TÍPUSA

A Hivatal informatikai rendszereinek elérésére használható hozzáférés szintjei:

1. **Névre szóló felhasználói hozzáférés** keretében a felhasználó külön, saját névre szóló, más által nem használt, kizárólag a munkája ellátása miatt elengedhetetlen jogosítványokkal rendelkezik az informatikai és telekommunikációs rendszerekhez és azok erőforrásaihoz, a szervezeti folyamatok ellátásához kapcsolódó feladatok elvégzéséhez.
2. **Névre szóló rendszergazdai hozzáférés** esetén, a rendszergazdai jogosítványt a rendszergazda a saját nevére szóló, kizárólagosan általa használt, megfelelő rendszergazdai jogkörrel felruházott felhasználói azonosító segítségével lehet használni. A rendszergazdai jelszavak minimális hossza 15 karakter. A hozzáférést csak a privilegizált parancsok futtatásakor szabad használni. A hozzáféréshez be kell állítani a kétténye zős hitelesítést.

3. **Nem névre szóló rendszergazdai hozzáférés** a nem személyhez köthető adminisztrátori jogosultságú (pl: root, superuser, admin stb.) azonosító ne legyen napi használatban, az csak olyankor használható, amikor elengedhetetlen (pl: vészhelyzet). A rendszergazdai jelszavak minimális hossza 15 karakter. A hozzáférést csak a privilegizált parancsok futtatásakor szabad használni. Jelentős biztonsági osztályba sorolt rendszerek esetén a hozzáféréshez beállított jelszavak csak egyszer használhatók, a rendszernek ki kell kényszerítenie a kötelező jelszó cserét minden egyes belépéskor.
4. **Nem névre szóló speciális hozzáférés** (technikai hozzáférés) esetén, speciális, csak célfeladat ellátáshoz szükséges jogosultsággal rendelkező hozzáférés lehet használni. (pl adatmentő rendszer működéséhez szükséges technikai hozzáférés) Ezen technikai hozzáféréseket csak akkor szabad alkalmazni, ha az adott háttérfolyamat más módon nem hajtható végre. A technikai hozzáférés kialakítása során gondoskodni kell:
    - felhasználó vagy informatikus ne tudjon bejelentkezni a technikai hozzáféréssel alkalmazásba vagy operációs rendszerbe,
    - a technikai hozzáféréshez tartozó jelszó legalább 15 karakter hosszú legyen,
    - a hozzáféréshez tartozó jelszó kisbetűt, nagybetűt, számot és speciális karaktert egyaránt tartalmazzon,
    - a hozzáféréshez tartozó jelszót zárt borítékban páncélszekrényben kell őrizni,
    - a hozzáféréshez tartozó jelszót, évente le kell cserélni,
    - kiemelten figyelni kell, a technikai felhasználóval történő bejelentkezéseket, adathozzáféréseket,
    - a technikai felhasználóval történő minden jogosulatlan hozzáférés, vagy bejelentkezés incidensnek minősül,
    - lehetőség szerint le kell tiltani a technikai hozzáféréssel grafikus vagy interaktív felületre történő bejelentkezést.

A nem személyhez köthető adminisztrátori azonosítókat és jelszavakat lezárt és az informatikus által aláírt borítékban a jegyző őrzi zárt szekrényben.

A borítékba úgy kell elhelyezni a jelszavakat, hogy azok ne legyenek „átvilágíthatóak", felbontás nélkül ne legyenek olvashatóak.

A borítékokra kívül rá kell írni az utolsó módosítás dátumát és a megbontás okát (pl. audit, vagy pl. jogosult távolléte miatti vezetői bontás), ilyen eseteket követően a jelszavakat le kell cserélni.

6.2. SZOFTVEREK KEZELÉSÉNEK SZABÁLYAI

6.2.1. OPERÁCIÓS RENDSZER SZINTŰ HOZZÁFÉRÉS ELLENŐRZÉS

Az informatikai infrastruktúrában olyan operációs rendszereket kell alkalmazni, amely a biztonságpolitikát legalább a következő területeken támogatja:

- Account-politika, amely meghatározza a felhasználó által karbantartott jelszavakkal kapcsolatos követelményeket,
- Felhasználói jog politika, amely meghatározza, hogy a felhasználókat (felhasználói csoportokat) milyen jogok illethetik meg és

- Audit-politika, amely meghatározza azt, hogy milyen informatikai eseményekről készüljön napló.

Központilag kell ellátni legalább az alábbi biztonság-kezelési funkciókat:

- Az operációs rendszerek adminisztrációja,
- Az rendszerprogramok központi installálása és konfigurálása,
- Valamennyi log-fájl archiválása,
- Jogosultságmenedzsment stb.

6.2.2. SZOFTVEREK TELEPÍTÉSE, HASZNÁLATA

A Hivatal által üzemeltetett rendszerprogramok, illetve a felhasználói programok letöltését, telepítését a szerverekre és munkaállomásokra kizárólag az erre feljogosított informatikus végezheti el. A felhasználók semmilyen szoftvert, alkalmazást nem telepíthetnek a munkaállomásaikra. Telepítési jogosultságot a jegyző engedélyezhet.

A felhasználó új alkalmazások telepítését, vagy a meglévő alkalmazásokat illető jogosultság változást az adatgazda vagy jegyző engedélyével igényelhet. A jegyző jogosult az igény felülvizsgálatára, és ha szükséges, biztonsági okból annak elutasítására.

A felhasználó a számítógépre telepített alkalmazásokat a felhasználói leírás szerinti módon, szakszerűen köteles használni.

A Hivatal informatikai rendszerében lévő szoftvereket csak a Hivatal munkatársai használhatják. Az informatikai rendszereket csak olyan személy használhatja, aki az adott szoftver használatát illetően képzésben részesült, illetve a használat módjáról kellő ismeretekkel és jártassággal rendelkezik. Ennek hiányában a szoftver csak olyan személy felügyelete mellett használható, aki rendelkezik ezekkel a feltételekkel és a szoftver rendeltetésszerű használatát illetően felelősséget vállal a felügyelete alatt dolgozó munkatárs munkájáért.

A szoftver használata során a felhasználó a szoftverek rendszer beállításait (kiszolgáló adatok, adatbázis információk, licence adatok, könyvtár útvonalak, stb.) nem módosíthatja, a szoftvereket nem törölheti és azokról másolatot nem készíthet. Ettől eltérni csak a jegyző engedélyével lehet.

A telepített szoftverekre előírt felhasználási előírásokat megsértő munkatárs munkajogi, polgári jogi és büntetőjogi felelősséggel tartozik.

6.2.3. ALKALMAZÁS SZINTŰ HOZZÁFÉRÉS ELLENŐRZÉS

Az információs rendszer logikai védelme az egyes funkcionális rendszerelemek (hardver, szoftver kommunikációs elemek stb.) által biztosított funkciókkal, tulajdonságokkal, képességekkel, továbbá az alkalmazott eljárásokkal, módszerekkel és/vagy biztonsági eszközökkel, algoritmusokkal, megoldásokkal, de - legfőképpen - ezek összhangjával biztosítható.

Az informatikai rendszer logikai védelmével kapcsolatban az alábbi követelményeket kell alkalmazni:

- Olyan architektúrát kell kialakítani, amely külön kezeli, illetve valósítja meg a kommunikációs, authentikációs és authorizációs, valamint az alkalmazás rétegeket.
- Biztosítani kell, hogy a központi rendszer egyetlen eleme sem legyen kihagyható vagy megkerülhető a rendszer felhasználói számára.

Amennyiben a szoftver alkalmas központi hitelesítő rendszerrel kommunikálni és azon keresztül hitelesíteni a felhasználót, úgy az egyszerűbb jogosultság kezelés megvalósítása érdekében az informatikai rendszereket össze kell kapcsolni. (pl.: Active Directory, LDAP, stb.)

6.3. MOBIL ESZKÖZÖK HASZNÁLATA ÉS TÁVMUNKA

A Hivatal hálózatában eseti távmunka végzést a jegyző engedélyezhet a megfelelő IT biztonság biztosítása mellett, írásbeli kérelem alapján. A Hivatal hálózatában távmunka végzés minden mobil informatikai eszközzel (laptop, notebook) rendelkező munkavállaló részére engedélyezett.

A Hivatal hálózatához kapcsolódásra képes mobil eszközökhöz (pl. notebook) kapcsolódó általános szabályok:

- külön biztonsági oktatásban kell részesülnie annak, aki ilyen eszközt fog használni, mielőtt az eszközt használatba veszi,
- a beépített merevlemezes egységen a kiemelten védendő adatokat kódolva kell tárolni,
- a Hivatal által biztosított mobil eszközt csak a munkatárs használhatja, aki az eszközt munkavégzésre megkapta,
- a Hivatal által biztosított mobil eszközt csak Hivatali munkavégzésre lehet használni,
- a 3.3.1 Felügyelet nélkül hagyott számítógépek fejezetben meghatározottak szerint kötelező az időzár (time-out) beállítása,
- a Hivatal irodáján kívül használt mobil eszközök védelmét 4.3.8 Eszközök védelme irodán kívül fejezetben meghatározottak szerint kell biztosítani,
- a Hivatal által biztosított mobil eszközökön található adatok mentéséről a 3.3.2 Rendszer-független mentési előírások felhasználók számára fejezet szerint kell eljárni,
- a Hivatal által biztosított mobil eszközökön tűzfal és vírusvédelmi szoftvernek kell működnie, a 5.3.2 Vírusvédelmi előírások fejezetben foglaltaknak megfelelően.

A Hivatal informatikai rendszereinek eléréséhez kialakított távoli hozzáférés használatához, a felhasználók részére felhasználói segédletet kell készíteni, amely tartalmazza a csatlakozáshoz, a távoli elérés használatához, és a kapcsolat lebontásához szükséges technikai ismereteket.

A munkatársak által használt céges mobilkészüléket (okostelefon, tablet) a Hivatal biztosítja, annak tulajdonát képezi, így minden, a Hivatal által előírt ellenőrzés és korlátozás, amely a felhasználó által elfogadásra került érvényesíthető. Az okostelefon, tablet használata során az alábbi adatvédelmi előírásokat kell betartani:

- PIN kódos vagy jelszavas képernyőzárat kell alkalmazni,
- a Hivatal által biztosított eszköz belső tárhelyét titkosítással kell védeni,
- a Hivatal által használt vírusvédelmi alkalmazást kell telepíteni és be kell kapcsolni a rendszer nyomon követési és távoli hozzáférést biztosító moduljait,
- tilos az eszközön magáncélú adatok tárolása, kezelése, (pl: privát fényképek vagy email kezelése és tárolása)
- az eszköz menedzseléséhez szükséges felhasználói hozzáférést (Apple, Google vagy Microsoft account) az informatikusnak kell létrehoznia, a hozzá tartozó jelszót borítékban kell őrizni, a felhasználónak átadni tilos,
- a telefonra csak a hivatalos alkalmazásboltból szabad alkalmazásokat telepíteni.

Az eszköz elvesztése, eltulajdonítása esetén a 4.3.9 Mi a teendő, ha az eszközt eltulajdonították fejezetben foglaltak szerint kell eljárni.

Távoli munkavégzés csak biztonságos kapcsolatokon keresztül történhet, a 6.3.1Távoli felhasználói hozzáférés a Hivatal hálózatához illetve 6.3.2 Felhasználói hozzáférés a Hivatal szolgáltatásaihoz fejezetek szerint.

A felhasználó köteles a Hivataltól kapott mobil eszközt lehetőleg hetente (de hosszabb távollét esetén lehetőleg havonta) a Hivatal hálózatához csatlakoztatni abból a célból, hogy a biztonsági és vírusvédelmi beállítások frissülhessenek, megőrizve ezzel a biztonság integritását.

A felhasználó az általa használt mobil eszközt az internetes szolgáltatások elérése céljából vezeték nélküli hálózathoz csak jegyzői engedéllyel csatlakoztathatja legalább WPA2-PSK kódolással védett vezeték nélküli hálózathoz. A nem megfelelő szinten titkosított, illetve nyílt hálózati kapcsolatok használata nem engedélyezett.

A munkatárs saját tulajdonában álló okostelefon használata esetén a jelen pontban írt előírásokat akkor kell alkalmazni, ha azon céges adatok tárolásra kerülnek (levelezés, fájlok, stb.).

A Hivatalon belül az információk átadása az alábbi módszerekkel történhet:

- értekezletek, megbeszélések,
- elektronikus levelezési rendszerben küldött üzenetek,
- megosztott mappák.

Az értekezlet(ek)ről szükség esetén feljegyzés/jegyzőkönyv készül, amelyek esetében minden munkatárs saját felelőssége, hogy az értekezleten elhangzott információkat bizalmasan kezelje, munkája során alkalmazza, és a feladatokat végrehajtsa.

6.3.1. TÁVOLI FELHASZNÁLÓI HOZZÁFÉRÉS A HIVATAL HÁLÓZATÁHOZ

A Hivatal informatikai erőforrásait, valamint a tárolt adatokat, a Hivatal irodáján kívülről csak titkosított adatcsatornán keresztül lehet elérhetővé tenni, a Hivatal által meghatározott és felügyelt technikai eszközzel.

A távoli hozzáféréshez használt technikai megvalósítást az informatikusnak a ***Rendszerdokumentációban*** le kell dokumentálnia. A dokumentációnak tartalmaznia kell:

- távoli hozzáférés internet felöli elérhetőségét (IP cím, URL, domain, stb),
- távoli hozzáférésre vonatkozó esetleges korlátozásokat (pl: GeoIP szűrés),
- távoli eléréshez használt hardver, szoftver megvalósítás beállításait (pl: port, protokoll, kliens eszközre telepítendő szoftver, stb.),
- hitelesítéshez használt technikai megvalósítás, kapcsolódó rendszerek (pl LDAP kapcsolat),
- távoli hozzáférés használatával elérhető erőforrások.

A szükséges hozzáféréseket az informatikus állítja be, a jegyző engedélye alapján.

A távoli hozzáférések használatakor a magas biztonsági kockázat miatt, kétfaktoros hitelesítést kell alkalmazni.

A távoli eléréshez csak a Hivatal által biztosított eszköz használható, más eszközök csatlakozását még helyes felhasználónév és jelszó esetén is technikai eszközzel meg kell akadályozni. (pl: tanúsítvány alapú eszköz hitelesítés)

Távoli munkavégzés esetén a távoli hozzáférést biztosító eszközt úgy kell beállítani, hogy:

- a bejelentkezéstől számított 4 óra elteltével ismételten hitelesítést kérjen a felhasználótól (session time beállítás),
- a távoli hozzáférés 10 perc inaktivitás után bontsa le, jelentkeztesse ki a felhasználót.

A távoli hozzáféréseket rendszeresen, évente legalább 1 alkalommal felül kell vizsgálni.

Távoli karbantartást, vagy hibajavítást csak az informatikus végezhet, külső szolgáltató esetén az informatikus felügyelete mellett végezhető.

Tilos a távmunkához használt eszközt munkavégzés ideje alatt más célra használni.

6.3.2. FELHASZNÁLÓI HOZZÁFÉRÉS A HIVATAL SZOLGÁLTATÁSAIHOZ

A Hivatal által használt szolgáltatások és a tárolt adatok SSL védett kapcsolaton keresztül érhetőek el. (pl: HTTPS)

A szükséges hozzáféréseket az informatikus és/vagy a szolgáltató állítja be, a jegyző engedélye alapján. Szolgáltatás esetén az adatgazda igényli meg a szolgáltatótól a jogosultság beállítását.

A távoli hozzáférések esetén kötelező a többtényezős hitelesítés alkalmazása. (felhasználónév + jelszó + token vagy felhasználónév + jelszó + tanúsítvány)

A hozzáféréseket rendszeresen, évente legalább 1 alkalommal felül kell vizsgálni.

6.3.3. A HORDOZHATÓ ESZKÖZÖK HASZNÁLATBA VÉTELE

A jogosult személyek a gépet tartozékokkal és szoftverekkel együtt veszik át az informatikustól, visszaszolgáltatási kötelezettséggel.

Átadáskor az informatikus a működőképes hordozható számítógép mellett a tartozéklistában felsorolt kiegészítőket, a munkavégzéshez szükséges telepített szoftverekkel együtt adja át.

6.3.4. ESZKÖZÖK VISSZASZOLGÁLTATÁSA

Amennyiben a munkatárs a továbbiakban nem kívánja, vagy nem jogosult használni az eszközt, vissza kell szolgáltatnia az informatikusnak, és értesíteni kell a jegyzőt.

Az eszközök raktárba való visszavételének lépései:

- a gépnek és tartozékainak tételes átvétele,
- az észlelt hibák jegyzőkönyvbe vétele,
- a gépen lévő adatok törlése, vagy megfelelő helyre való mentése.

6.4. ELTÉRÉS AZ ÁLTALÁNOS KÖVETELMÉNYEKTŐL

Az IBSZ-ben általános jelleggel meghatározott biztonsági követelmények teljesítésétől az informatikus felmentést kérhet, ha az alábbi feltételek egyidejűleg fennállnak:

- a követelmények teljesítését a Hivatal rendelkezésére álló hardver és szoftver technológia nem teszi lehetővé, és
- felmérte a munkafolyamatban fennálló azon kockázatokat, amelyek a biztonsági kontrollok elhagyásából fakadnak, és
- a biztonsági kontrollok kialakításának költsége nem áll arányban a biztonsági kontrollok elhagyásából fakadó kockázatokkal.

Az eltérést a biztonsági követelményektől a jegyző engedélyezheti.

7. INFORMATIKAI BIZTONSÁGI INCIDENSEK KEZELÉSE

Az észlelt információvédelmi eseményeket, és a feltételezett gyengeségeket írásban, bizalmasan kell bejelenteni a ***Biztonsági Eseménykezelési eljárásrendben*** megfogalmazottak szerint.

8. MŰKÖDÉS FOLYTONOSSÁG BIZTOSÍTÁSA

A Hivatalnak rendelkeznie kell a működés folytonosság fenntartásához és javításához szükséges eljárási és működtetési dokumentációkkal. ***(Informatikai Katasztrófaterv, Üzletmenet-folytonossági terv)***

A működésfolytonossági tervek elkészítését, illetve módosítását követően tesztelni kell a dokumentumokban foglaltakat. A jegyző által megbízott személy tervezi meg, koordinálja és dokumentálja a teszteket.

A sikeres tesztelés után meg kell tartani a működésfolytonosság biztosításában érintett személyek részére a szükséges oktatásokat.

A működésfolytonossági tervek felülvizsgálata akkor szükséges, ha a kockázatok, az üzleti követelmények vagy az informatikai rendszerek változnak.

9. KÖVETELMÉNYEKNEK VALÓ MEGFELELÉS

9.1. JOGI KÖVETELMÉNYEK

9.1.1. JOGSZABÁLYOK

Vonatkozó jogszabályok:

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról,
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról,
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről,
- az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv),
- 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 („GDPR"),
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról („Infotv").

Ha a Hivatal munkatársa az informatikai biztonsági szabályokat megszegve a Hivatalnak kárt okoz, a jegyző kártérítési eljárást kezdeményez vele szemben.

9.1.2. SZOFTVEREK JOGTISZTASÁGA

A Hivatal informatikai rendszereiben csak központilag telepített, engedélyezett és felügyelt, jogtiszta szoftverek használhatók.

A Hivatalnak rendelkeznie kell egy szoftver listával (***Engedélyezett szoftverek listája***), ami definiálja a Hivatal számítógépeire telepíthető és használható szoftvereket. A szoftverlistában nem szereplő alkalmazások telepítése előzetes vizsgálathoz és a jegyzői engedélyéhez kötött. Csak a munkavégzéshez szükséges szoftverek telepíthetők.

Az ***Engedélyezett szoftverek listája*** alapján az informatikusnak évente egy alkalommal szoftver felülvizsgálatot és licenc ellenőrzést kell végeznie. A jogosulatlanul telepített szoftvereket, illetve azokat a szoftvereket, amelyekhez a Hivatal nem rendelkezik licenccel, el kell távolítania és erről jegyzőkönyvet kell felvennie, amit a jegyzőnek el kell juttatni. A felülvizsgálat során, ha szükséges, módosítani kell az ***Engedélyezett szoftverek listáját***. A vizsgálatok elvégzéséhez lehetőség szerint automatizált eszközt (automatikus hardver-szoftver leltár készítő eszköz) kell használni.

A Hivatal által birtokolt és használt szoftverek telepítő készleteit, telepítő kódjait tilos kivinni, átadni, másolni vagy mások részére hozzáférhetővé tenni, kivéve, ha erről a Hivatallal kötött szerződések másként rendelkeznek.

A Hivatal tulajdonában és használatában lévő számítógépek csak Hivatal által engedélyezett és nyilvántartott szoftvereket tartalmazhatják.

A szoftverek frissítése esetén a jogilag tisztán birtokolt szoftverek gyártói által biztosított javító készleteket kell használni.

Az ingyenesen használható és próba licencek esetében a gyártó licencszerződésében meghatározottak szerint kell eljárni.

Próbaverzióval rendelkező szoftver licencek használatát kerülni kell.

9.1.3. INFORMATIKAI DOKUMENTÁCIÓK VÉDELME

A fontosabb dokumentációk másolásáról és biztonságos tárolásáról gondoskodni kell:

- Informatikai Biztonsági Szabályzat és mellékletei (sablon és kitöltött dokumentumok egyaránt)
- Informatikai Katasztrófaterv
- Informatikai rendszerek biztonságával, használatával kapcsolatos jegyzői utasítások (pl: URL szűrési utasítás, adathordozó használat szabályozás, Engedélyezett szoftverek listája, stb.)
- Informatikai rendszerrel kapcsolatos nyilvántartások, jegyzőkönyvek, (pl: jogosultság kiosztási nyilvántartás, incidens kezelési jegyzőkönyvek, stb.)
- Informatikai rendszerrel kapcsolatos audit jelentések, riportok, (pl.: jegyzőkönyvek)
- Informatikai rendszer dokumentációi, rendszertervek, hálózati és adatkapcsolati ábrák, leírások, üzemeltetői és felhasználói kézikönyvek, utasítások (pl: rendszergazdai dokumentáció, stb.).

A rendszerről készült dokumentációkat bizalmasan kell kezelni. A készített dokumentumokat az informatikus őrzi.

Az installált rendszerszoftverek és az egyedinek tekinthető, a nem reprodukálható alkalmazói szoftverek referencia-másolatait biztonságosan kell tárolni.

Az auditok során készített jegyzőkönyveket, elemzéseket bizalmasan kell kezelni. A készített dokumentumokat a jegyző megbízottja őrzi.

9.1.4. TITKOSÍTÁSI ELŐÍRÁSOK

Az informatikusnak nyilvántartást kell vezetnie a felhasználóknak átadott titkosításhoz használt kulcsokról, visszavonáskor gondoskodnia kell a kulcsok megsemmisítéséről. Biztosítani kell a titkosításhoz használt kulcsok biztonságos előállítását, tárolását.

Az adatok titkosításához csak megbízható rejtjelező algoritmust alkalmazó eszközöket szabad használni. A megfelelő titkosítás elsősorban a következők használatát jelenti:

- csatolmányok tömörített formában való titkosítása, legalább 8 karakteres jelszóval (pl: 7Zip, PGP)
- mobil adathordozók esetében jelszóval kell védeni a hozzáférést, lehetőség szerint automatizáltan kell a titkosítást kikényszeríteni. (Pl: Bitlocker)

A bizalmasság és integritás védelmében alkalmazott rejtjelkulcsok (a szimmetrikus algoritmusok kulcsai) továbbítása az információs rendszerben (pl. a védett kulcsok időszakos cseréje miatt) csak védett csatornán keresztül történhet.

A titkosításhoz használt kulcsokat védeni kell, nem szabad harmadik személynek kiadni.

A mobil adathordozók és mobil informatikai eszközök esetén a teljes adathordozóra érvényes titkosítást kell alkalmazni. Amennyiben az adathordozón tárolt adatok az 1. bizalmassági szintbe tartozó informatikai rendszerbe kerülnek feldolgozásra (pl: fényképezőgépek memória kártyái) akkor az adathordozót nem szükséges titkosítással ellátni.

A Hivatal eszközein egységes titkosító szoftver megoldást kell használni.

A Hivatal számítógépein és a laptopjain a beépített adattároló eszköz (HDD, SSD) teljes tárterületét titkosítani kell. (Pl: Bitlocker). A titkosító szoftvert szerint úgy kell konfigurálni, hogy 5 sikertelen feloldási kísérlet után törölje az eszköz tartalmát, vagy csak a mesterkulcs feloldásával lehessen az eszköz zárolását feloldani.

A titkosításhoz használt algoritmusoknak és technikai megoldásoknak a kor technikai, technológiai színvonalához kell alkalmazkodnia. A megfelelő titkosítás kiválasztásakor figyelembe kell venni hazai és nemzetközi „best practice" megoldásokat, valamint a jogszabályi és hatósági elvárásokat.

A kriptográfiai eszközök azonosítóit és jelszavait (pl: Bitlocker mesterkulcs) páncélszekrényben, zárt borítékban kell tárolni. A boríték a jegyző utasítására bontható fel.

A Hivatal által üzemeltetett informatikai rendszerben csak a Nemzeti Média- és Hírközlési Hatóság bizalmi szolgálatásokkal kapcsolatos nyilvántartásaiban szereplő hitelesítésszolgáltatók szolgáltatásai alkalmazhatók.

Elektronikus aláírást kizárólag a jegyző engedélyével lehet alkalmazni. Az elektronikus aláírás eszközeinek és jelszavainak kezeléséért és megőrzéséért az alkalmazó felhasználó a felelős.

A hitelesítési rendszer kialakítása és a rendszer nyilvántartása az informatikus feladata.

9.2. INFORMATIKAI RENDSZER FELÜLVIZSGÁLATA

9.2.1. FELÜLVIZSGÁLATI ELŐÍRÁSOK

Az informatikai ellenőrzések területei:

- Környezeti veszélyek - pl.: természeti károk, tűz stb. Fizikai veszélyek - lopás, rongálás, fizikai betörés.
- Informatikai veszélyek - vírusok, számítógépes betörés stb.
- Humán veszélyek - szabotázs, gondatlanság, tudatlanság, felelőtlenség stb. Szervezeti veszélyek - szervezeti problémák, irányítási gondok stb.
- Szervezeti veszélyek - szervezeti problémák, irányítási gondok stb.

Az informatikai ellenőrzések rendszere a Hivatalnál:

- Alapszintű ellenőrzés: az informatikus által.
- Középszintű ellenőrzés:
  - informatikai biztonsági felelős
  - belső ellenőr,
  - jegyző,
- Felsőszintű ellenőrzés: hatóságok ellenőrzései, felügyeleti kontrolja.

A Hivatal alkalmazásainak auditálása az érintett szervezeti egységek vezetőivel egyeztetve folytatható úgy, hogy az ne veszélyeztesse azoknak a biztonságát.

A vonatkozó jogszabályok alapján, a jogszabályok által előírt gyakorisággal el kell végeztetni az informatikai rendszer auditálását, az erre feljogosított szervezettel.

Az informatikai rendszerek biztonsági állapotáról a jegyző által megbízott szervezet vagy az informatikai biztonsági felelős által elvégzett biztonsági ellenőrzésekkel és értékelésekkel kell

meggyőződni. Az informatikai rendszerek biztonsági állapotáról jegyzőkönyvet kell készíteni és az informatikai biztonsági felelőssel véleményeztetni kell.

A szakszerűséget, tárgyilagosságot és függetlenséget biztosítani kell a biztonsági ellenőrzéseknél a résztvevők - külső cégek és (vagy) belső személyek - kiválasztásával.

Az informatikai rendszer biztonságos működésének teljes vagy részleges technikai ellenőrzését (pl: sérülékenység vizsgálat, konfiguráció elemzés, behatolás vizsgálat, stb.) évente el kell végezni.

A megfelelő feltételeket, például személyeket, infrastruktúrát, eszközöket, hatásköröket stb. biztosítani kell a rendszeres biztonsági ellenőrzésekhez

Az ellenőrzések során feltárt hiányosságokat az informatikai biztonsági felelős értékeli, majd tájékoztatja a jegyzőt.

9.2.1.1. INFORMATIKAI KOCKÁZATELEMZÉS

Az információk kiszivárgásának megelőzése érdekében a Hivatal rendszeres kockázatelemzést alkalmaz, így azonosítja az informatikai rendszer esetleges biztonsági kockázatait és jogszabályi nem megfelelősségét.

A kockázatelemzés során az egyes veszélyforrások által képviselt kockázatokat kell megállapítani, illetve feltárni. A kockázat meghatározása a veszély megvalósulásának valószínűsége és az okozható kár, vagy más nézőpontból az adott veszélyt képviselő sérülékenység kihasználhatósága és ennek hatása alapján történik.

A kockázatok azonosítása után cselekvési tervet készít és a kockázatnak megfelelő arányú védelmi intézkedéseket vezet be.

Az kockázatelemzést rendszeresen, kétévente el kell végezni az ***Informatikai Kockázatelemzési és kezelési eljárásrend*** szerint.

9.2.1.2. SÉRÜLÉKENYSÉG VIZSGÁLAT

Új rendszer bevezetése, meglévő rendszer főverzió frissítése esetén, de legalább évente sérülékenységvizsgálatot kell lefolytatni. A vizsgálat hatókörét az informatikus és a jegyző együttesen határozzák meg.

9.2.1.3. TECHNIKAI VIZSGÁLATOK

A rendszer sebezhetőségének azonosítása, kezelése és ellenőrzése érdekében rendszeresen felül kell vizsgálni a beállításokat, illetve a működést.A távoli munkavégzéséhez, illetve telephelyek összekötéséhez használt fizikai (pl: optikai hálózat, béreltvonal, stb.) vagy logikai összeköttetés (pl: Site2Site VPN, client-site VPN, stb.) beállításait, illetve a hozzájuk tartozó tűzfal és routing szabályokat évente egy alkalommal felül kell vizsgálni, a szükséges biztonsági intézkedéseket alkalmazni kell. (pl: új titkosító algoritmusok alkalmazása, elavult technológiák letiltása)

Technikai ellenőrzés, ***Informatikai Katasztrófaterv*** tesztelése, keretében meg kell bizonyosodni az informatikai rendszer által biztosított rendelkezésre állási idők megfelelősségéről. A tesztelést legalább 2 évente el kell végezni.

9.2.2. CSELEKVÉSI TERV ÉS MÉRFÖLDKÖVEI

Az informatikai biztonsággal kapcsolatos felmérések és felülvizsgálatok során megállapított hiányosságok kezelésére minden esetben cselekvési tervet kell készíteni. A ***Cselekvésiterv*** tartalmazza a felmerült hiányosságok kezeléséhez szükséges konkrét feladatokat, felelősségi köröket és a végrehajtási határidőket. A ***Cselekvésitervben*** szerepelő határidőknek illeszkedniük kell, az ***Informatikai Kockázatelemzési és kezelési eljárásrendben*** a kockázatok kezelésére meghatározott időhöz.

Az intézkedési tervet az informatikai biztonsági felelős készíti el, és a jegyző hagyja jóvá. A ***Cselekvésitervben*** meghatározott feladatokhoz (elsősorban konfiguráció módosítások, logikai védelmi intézkedések, szoftver csere-frissítés, stb.) esetileg szükség lehet implementációs tervre, amit az informatikus készít. Az implementációs tervet az informatikai biztonsági felelősnek véleményeznie kell.

A ***Cselekvésitervben*** meghatározott célokhoz határidőket kell rendelni, amelyek segítségével nyomon követhető a ***Cselekvésitervben*** meghatározott feladatok végrehajtásának előrehaladása.

A ***Cselekvésitervben*** meghatározott feladatokhoz felelőst kell kijelölni, aki:

- vagy elvégzi a meghatározott feladatot,
- vagy felügyeli, koordinálja a feladat végrehajtását.

A jegyző felelőssége, hogy a ***Cselekvésitervben*** meghatározott feladatok elvégzéséhez szükséges személyi, tárgyi, pénzügyi feltételeket biztosítsa.

A ***Cselekvésitervben*** meghatározott feladatok végrehajtását az informatikusnak naprakészen nyomon kell követni és a határidők lejárata előtt 1 héttel, írásban tájékoztatni kell a jegyzőt és az informatikai biztonsági felelőst a feladat állapotáról. A tájékoztatás történhet jegyzőkönyvben vagy emailben.

A ***Cselekvésitervet*** az informatikai biztonsági felelős rendszeresen, 3 havonta felülvizsgálja és írásban tájékoztatja a jegyzőt a ***Cselekvésitervben*** megfogalmazott feladatok állapotáról.

10. MELLÉKLETEK

1. számú melléklet – Biztonsági Osztályba Sorolási eljárásrend
2. számú melléklet – Selejtezési Szabályzat
3. számú melléklet –Jogosultság kiosztási nyilvántartás
4. számú melléklet – Besorolási ív
5. számú melléklet - Alkalmazotti nyilatkozat
6. számú melléklet – Adat besorolási kérelem
7. számú melléklet – Munkahelyi környezet létrehozása/megszüntetése
8. számú melléklet – Felhasználói jogosultság igénylő lap
9. számú melléklet – Mentési utasítás
10. számú melléklet - Géptermi napló
11. számú melléklet - Archiválási napló

11. KAPCSOLÓDÓ SZABÁLYZATOK, VEZETŐI UTASÍTÁSOK

- Informatikai Beszerzési Eljárásrend
- Informatikai Katasztrófaterv
- Üzletmenetfolytonossági terv
- Informatikai Kockázatelemzési Eljárásrend
- Informatikai Biztonság Elemzési Eljárásrend
- Biztonsági Eseménykezelési Eljárásrend
- Vagyonvédelmi kamera szabályzat
- Rendszerdokumentáció
- Rendszerfejlesztési terv
- Adathordozó használat jegyzői utasítás
- Mobil eszközök kivitele jegyzői utasítás
- URL szűrés jegyzői utasítás
- Távmunka jegyzői utasítás

12. EGYÉB DOKUMENTUMOK

- Adatgazdai kinevezések
- Engedélyezett szoftverek listája
- Informatikai karbantartási, biztonsági tesztelési terv
- Informatikai Fejlesztési Terv

Informatikai Biztonsági Szabályzat 1. számú melléklete

Biztonsági Osztályba Sorolási eljárásrend

Dokumentum változástörténet

Dátum	Szerző	Verzió	Módosítás tárgya
2021.08.04.	Biró Gergely Ganev Attila	1.0	Átadott verzió
2023.06.27	Biró Gergely Ganev Attila	1.1	NKI észrevételek alapján felülvizsgált verzió
2025.07.29	Biró Gergely Ganev Attila Fazekas Viktória	1.2	Jogszabályi változások alapján felülvizsgált verzió
2025.06.09	Biró Gergely Ganev Attila Kereső Krisztina	1.3	Jogszabályi változások alapján felülvizsgált verzió

Ellenőrizte

Dátum	Név	Verzió	Aláírás

Jóváhagyta

Dátum	Név	Verzió	Aláírás
2026.07.07	Kovács Éva		Kovács Éva

POLGÁRMESTERI HIVATAL 1. JÁSZ-NAGYKUN-SZOLNOK VÁRMEGYEI KENDERES

1. BIZTONSÁGI OSZTÁLYBA SOROLÁS

1.1. AZ ELJRÁSÁREND CÉLJA, HATÁLYA

Az eljárásrend célja egy olyan osztályozó rendszer létrehozása, amely a Hivatal által használt elektronikus információs rendszereket, a rendszerekben tárolt adatok fontossága és védelmi szükséglete alapján, megfelelően osztályozza, és ezzel megfelelő védelmi, kezelési intézkedéseket foganatosít megóvásuk érdekében.

Az Eljárásrend személyi hatálya megegyezik az ***Informatikai Biztonsági Szabályzat*** Az IBSZ hatálya fejezetében foglaltakkal.

Az Eljárásrend tárgyi hatálya megegyezik az ***Informatikai Biztonsági Szabályzat*** Az IBSZ hatálya fejezetében foglaltakkal.

Az Eljárásrend területi hatálya megegyezik az ***Informatikai Biztonsági Szabályzat*** Az IBSZ hatálya fejezetében foglaltakkal.

Az Eljárásrend időbeli hatálya:

- az Eljárásrend az aláírás napját követő első munkanapon lép hatályba. A dokumentumba foglalt feladatok és szabályok ezen időponttól alkalmazandók azzal, hogy a hatályba lépéskor folyamatban lévő ügyekre is alkalmazni kell.
- az Eljárásrend visszavonásig hatályos.

2. ADATOK OSZTÁLYOZÁSA

2.1. AZ ADATOK OSZTÁLYOZÁSI RENDSZERE

A biztonsági osztályba sorolás szabályainak meghatározásához a vonatkozó jogszabályi előírásokat vettük alapul, amelyek az informatikai biztonságot annak három alapvető összetevőjén keresztül határozzák meg:

- **Bizalmasság**: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról,
- **Sértetlenség**: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható,
- **Rendelkezésre állás**: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

Az adatok besorolása során e három dimenzió mentén határozhatóak meg az elektronikusan kezelt és/vagy tárolt információk biztonsági követelményei.

2.1.1. BIZALMASSÁGI KATEGÓRIÁK MEGHATÁROZÁSA

A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet 1. melléklete alapján az adatok bizalmassági kategóriáinak meghatározása a következő:

- 1 szintű adatok bizalmasságának sérülése vagy elvesztése nem, vagy csak elhanyagolható mértékű anyagi vagy reputációs veszteséget okoz (pl: jogszabály által nem védett vagy nyilvánosan hozzáférhető adatok);
- 2 szintű adatok bizalmasságának sérülése vagy elvesztése csak kis mértékben okozhat anyagi vagy reputációs veszteséget (pl: személyes adatok, email címek, elérhetőségek, stb);
- 3 szintű adatok bizalmasságának sérülése vagy elvesztése jelentős anyagi vagy reputációs veszteséget okoz (pl: különleges adatok, jogszabállyal védett adatok, üzleti titok, stb.);
- 4 szintű adatok bizalmasságának sérülése vagy elvesztése kritikus mértékű anyagi vagy reputációs veszteséget okoz (pl: nagy értékű üzleti titok, szolgálati titok, stb.).

2.1.2. A SÉRTETLENSÉGI ÉS RENDELKEZÉSRE ÁLLÁSIKATEGÓRIÁK MEGHATÁROZÁSA

A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet 1. melléklete alapján az adatok sértetlenség és rendelkezésre állási kategóriáinak meghatározása a következő:

- SR1 a sértetlenség vagy rendelkezésre állás nem kritikus. Az adatok sértetlenségének vagy rendelkezésre állásának sérülése vagy elvesztése a szervezetnek vagy más személynek nem, vagy csak elhanyagolható mértékben okozhat anyagi vagy reputációs vesztesége

- SR2 a sértetlenség vagy rendelkezésre állás kritikus. Az adatok sértetlenségének vagy rendelkezésre állásának sérülése vagy elvesztése a szervezetnek vagy más személynek jelentős, vagy kritikus mértékű anyagi vagy reputációs veszteséget okozhat.

2.2. AZ ADATOSZTÁLYOZÁS LEKÉPEZÉSE

A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet 1. melléklete tartalmazza az adatok besorolásának szabályait. Az adatok osztályozása alapján kell meghatározni az adat védelmi szintjét (Számított BSR érték). Az elektronikus információs rendszer biztonsági osztályának és az elektronikus információs rendszertől elvárt logikai védelem meghatározásakor figyelembe kell venni adat védelmi szintjére vonatkozó jogszabályi előírásokat.

Az adatok bizalmasság szerinti besorolása (B)	Az adatok sértetlenség és rendelkezésre állás szerinti összesített értéke (SR)	Számított BSR érték	EIR biztonsági osztály
1	1	2	Alap
1	2	3	Alap
2	1	3	Alap
2	2	4	Jelentős
3	1	4	Jelentős
3	2	5	Magas
4	1	5	Magas
4	2	6	Magas

3. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BESOROLÁSA

3.1. A BIZTONSÁGI OSZTÁLYOK MEGHATÁROZÁSA

A biztonsági osztályba sorolás szabályainak meghatározását biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 1. melléklete tartalmazza, az alábbiak szerint.

„Alap" biztonsági osztály

Az „alap" biztonsági osztályba tartozik minden olyan informatikai rendszer, amely olyan adatot kezel, ami

- jogszabály által nem védett,
- kevés személyes adatot kezelő, (nem teszi egyértelműen beazonosíthatóvá az érintetett)
- nyilvánosan hozzáférhető adatot tartalmaz.

Az adatok nyilvánosságra kerülése az érintett személyek, illetve a szervezet számára erkölcsi következménnyel jár, anyagi és jogi következmény nincs. Ilyen rendszer többek között a weboldal, közösségi oldal, közérdekű adatokat kezelő informatikai rendszerek, stb.

Az informatikai rendszerben tárolt adatok véletlen vagy rosszindulatú módosítása, illetve törlése a napi működési folyamatokat lényegesen nem befolyásolhatja, bizalomvesztés következhet be, a jogszabályi kötelezettségek elmaradhatnak.

„Jelentős" biztonsági osztály

A „jelentős" biztonsági osztályba tartozik minden olyan informatikai rendszer, amely olyan adatot kezel, ami

- olyan adatot kezel, ami minden alkalmazottnak és szerződéses munkatársnak korlátozás nélkül rendelkezésére áll, de nem publikus információ,
- jogszabállyal védett adatokat tartalmaz,
- üzleti titokként kezelt adatokat tartalmaz,
- nagy mennyiségben személyes adatokat tartalmaz,
- olyan személyes adatot tartalmaz, amely egyértelműen beazonosíthatóvá teszi az érintetett,
- kis mennyiségben tartalmaz különleges személyes adatot.

Az adatok nyilvánosságra kerülése az érintett személyek vagy szervezet számára hátrányos erkölcsi, jogi és anyagi következményeket von maga után. Ilyen rendszerek többek között a dokumentumkezelő, feldolgozó rendszer, a munkaügyi, pénzügyi, szociális adatokat tartalmazó rendszerek, a szervezet számára kritikus központi informatikai rendszerek, valamint a munkatársak jogosultságait kezelő rendszerek.

Az informatikai rendszerben tárolt adatok véletlen vagy rosszindulatú módosítása, illetve törlése a napi működési folyamatokat és jogszabályokban előírt határidőben valamint kellő minőségben történő teljesítését:

- közvetlenül, lényeges mértékben befolyásolhatja,
- jogi és/vagy anyagi következményekkel járhat.

„Magas" biztonsági osztály

A „magas" biztonsági osztályba tartozik minden olyan informatikai rendszer, amelyek kezelik:

- különleges adatokat,
- az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény szerint meghatározott, szolgálati titkokat,
- nemzeti adatvagyont,
- nagy értékű, a szervezet fennmaradását biztosító üzleti titkot.

A magas" biztonsági osztályba tartoznak azon rendszerek is, amelyeknek meghibásodása, nem megfelelő működése emberi élteket veszélyeztethet.

Az adatok nyilvánosságra kerülése vagy a rendszerek nem megfelelő az érintett személyek vagy szervezetek számára súlyos erkölcsi, jogi és anyagi következményeket von maga után. Ilyen rendszerek többek között betegek adatait kezelő rendszerek, emberi élet védelmét biztosító rendszerek, stb.

Az informatikai rendszerben tárolt adatok véletlen vagy rosszindulatú módosítása illetve törlése súlyos jogi és anyagi következményekkel járhat, mely a szervezet létét veszélyeztetheti.

3.2. AZ INFORMATIKAI RENDSZER RENDELKEZÉSRE ÁLLÁSI IGÉNYÉNEK BESOROLÁSI KATEGÓRIÁI

Az elektronikus információs rendszereinek, a Hivatal üzletmenete által elvárt, rendelkezésre állási kategóriái az alábbiak szerint kerültek meghatározásra:

1. **kategória**: Mindazon informatikai rendszerek, amelyeknél az elvárt helyreállítási idő (RTO) 72 óra, az elvárt helyreállítási pont 48 óra.
2. **kategória**: Mindazon informatikai rendszerek, amelyeknél az elvárt helyreállítási idő (RTO) 24 óra, az elvárt helyreállítási pont 8 óra.
3. **kategória**: Mindazon informatikai rendszerek, amelyeknél az elvárt helyreállítási idő (RTO) 8 óra, az elvárt helyreállítási pont 4 óra.

3.3. AZ INFORMATIKAI RENDSZER BESOROLÁSÁNAK ELJÁRÁSRENDJE

Minden informatikai rendszert, amely a Hivatalnál bevezetésre kerül be kell vonni a besorolási eljárásba. A besorolási eljárás végeredménye a ***Besorolási ív*** amelynek célja az informatikai rendszerek biztonsági besorolásának nyilvántartása. A ***Besorolási ív*** az IBSZ mellékletét képezi, a következő tartalommal:

- az informatikai rendszer megnevezése,
- az informatikai rendszer típusa,
- az informatikai rendszer biztonsági osztálya,
- az informatikai rendszer rendelkezésre állási besorolása,
- az informatikai rendszer elektronikus információs rendszeri minősége,
- az informatikai rendszerhez rendelt adatgazda neve;
- az informatikai rendszert üzemeltető szervezet neve,

- az informatikai rendszert támogató szervezet neve, elérhetősége,
- az informatikai rendszerben tárolt adattípusok felsorolása,
- az informatikai rendszerben keletkező adatok éves mennyisége,
- az informatikai rendszerben tárolt adatok bizalmassági besorolása,
- az informatikai rendszerben tárolt adatok sértetlenségi és rendelkezésre állási besorolása.

A ***Besorolási Ív*** **tartalmát** a jegyző hagyja jóvá és adja ki.

3.4. AZ ADATGAZDÁK SZEREPE ÉS FELELŐSSÉGE

Az adatgazdákat a jegyző jelöli ki.

Új informatikai rendszer bevezetése esetén az adatgazda köteles az informatikai rendszer biztonsági besorolását kérni az informatikai biztonsági felelőstől. A kérelmet írásban, az IBSZ mellékletét képező ***Adatbesorolási kérelem (6. számú melléklete)*** formanyomtatványon kell benyújtani a javasolt besorolások megjelölésével és indoklásával. A kérelem benyújtását követően az informatikai biztonsági felelős elvégzi az informatikai rendszer biztonsági osztályba sorolását, amit átad a jegyzőnek jóváhagyásra.

3.5. A BESOROLÁSI ÍV KARBANTARTÁSA

A ***Besorolási ív*** tartalmát az informatikai biztonsági felelős az IBSZ rendszeres évi felülvizsgálata során áttekinti, és szükség esetén elvégzi. Az újrabesorolási eljárásba az informatikai biztonsági felelős az érintett adatgazdákat bevonhatja.

A ***Besorolási ív***ben felsorolt egyes adatok újbóli besorolását a Hivatal bármely dolgozója, illetve a rendszerben tárolt adatok bármely adatgazdája kezdeményezheti. Az újrabesorolás kezdeményezését írásban, indoklással kell benyújtani a jegyzőnek.

A ***Besorolási ív*** módosításait minden esetben a jegyző hagyja jóvá és adja ki.

4. AZ ADATOK ÉS ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BESOROLÁSÁNAK LEKÉPEZÉSE

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 1. mellékletében, valamint Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet 1. mellékletében szereplő adat, illetve elektronikus információs rendszer biztonsági besorolására vonatkozó előírások közötti összefüggést az alábbi táblázat tartalmazza.

Biztonsági osztály	Rendelkezésre állás	Az adatok bizalmasság szerinti besorolása (B)	Az adatok sértetlenség és rendelkezésre állás szerinti összesített értéke (SR)	Számított BSR érték	Titkosítási elvárás	Az adatkezelés helyszínének meghatározása
„Alap" biztonsági osztály	1,2 kategória	1	1	2	Nem szükséges titkosítás	F1
		1	2	3	Nem szükséges titkosítás	F2
		2	1	3	Titkosítás szükséges	F2
„Jelentős" biztonsági osztály	2,3 kategória	2	2	4	Titkosítás szükséges	F3
		3	1	4	Titkosítás kötelező	F3
„Magas" osztály	3 kategória	3	2	5	Titkosítás kötelező	F4
		4	1	5	Titkosítás kötelező	F4
		4	2	6	Titkosítás kötelező	F4

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 2. melléklete tartalmazza a biztonsági osztályok által elvárt, az elektronikus információs rendszerre vonatkozó adminisztratív, logikai és fizikai elvárásokat. Az ***Informatikai Biztonsági Szabályzat*** tartalmazza a

jogszabályi elvárásoknak megfelelő szabályozást, ami alapján az egyes informatikai rendszerek védelméről gondoskodni kell.

4.1. AZ ADATKEZELÉS HELYSZÍNÉNEK MEGHATÁROZÁSA

A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet 1. melléklete alapján az adatkezelés helyszínének meghatározásai az alábbiak:

- F1
  A B és SR összesített értéke: 2
  Az F1 besorolású adatok – földrajzi korlátozás nélkül, – nem privát felhőszolgáltatás igénybevétele esetén korlátozás nélkül kezelhetők és tárolhatók.

- F2
  A B és SR összesített értéke: 3
  Az F2 besorolású adatok:
  - SR1 besorolású adatok esetén földrajzi korlátozás nélkül tárolhatók;
  - SR2 besorolású adatok esetén kizárólag EGT tagállam területén tárolhatók;

  Nem privát felhőszolgáltatás igénybevétele esetén:
  - EGT tagállam területén kívül kizárólag az igénybe vett szolgáltatás vonatkozásában harmadik fél általi, a kiberbiztonsági hatóság honlapján közzétett lista szerinti kiberbiztonsági tanúsítással, audittal vagy engedélyezéssel rendelkező (a továbbiakban: harmadik fél által tanúsított) nem privát felhőben tárolhatók;
  - EGT tagállam területén belül akár nem tanúsított nem privát felhőben is kezelhetők és tárolhatók.

  Magyarország területén kívüli adattárolás esetén egyidejűleg gondoskodni kell az adatnak Magyarország területén való rendelkezésre állásáról is. (pl: biztonsági mentéssel)

- F3
  A B és SR összesített értéke: 4
  Az F3 besorolású adatok kizárólag EGT tagállam területén belül, nem privát felhőszolgáltatás igénybevétele esetén:
  - harmadik fél által tanúsított nem privát felhőben, vagy
  - nem tanúsított nem privát felhőszolgáltatás igénybevétele esetén kizárólag Magyarország területén kezelhetők és tárolhatók.

  Magyarország területén kívüli adattárolás esetén egyidejűleg gondoskodni kell az adatnak Magyarország területén való rendelkezésre állásáról is. (pl: biztonsági mentéssel)

- F4
  A B és SR összesített értéke: 5 vagy 6
  Az F4 besorolású adatok kizárólag Magyarország területén (saját telephelyen), nem privát felhőszolgáltatás igénybevétele esetén:
  - harmadik fél által tanúsított privát felhőben vagy
  - kormányzati felhőben kezelhetők.

  Magyarország területén kívüli adattárolás esetén egyidejűleg gondoskodni kell az adatnak Magyarország területén való rendelkezésre állásáról is. (pl: biztonsági mentéssel)

Megismerési nyilatkozat

Az Informatikai Biztonsági Szabályzatban foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás
KIRÁLY KRISZTIÁN	MŰSZAKI ÜGYINTÉZŐ	2026. 07. 08.	
DARADICS LUJZA	TITKÁRSÁGI ÜGYIN.	2026.07.08	Daradics Lujza
BARTUCSEK KATALIN	SZOCIÁLIS ÜGYINTÉZŐ	2026.07.08.	Bartucsek Katalin
DR. FARKASNÉ MIKA MÓNIKA	ÁLLATORVOS	2026.07.08.	
DARNOSNÉ ÖRÖKÖS-TÓTH EDIT	PÉNZÜGYI ÜGYINTÉZŐ	2026.07.08.	Örökös-Tóth Edit
HAJTÓN ANIKÓ	PÉNZÜGYI ÜGYINTÉZŐ	2026.07.08	
NATYELKA-BESENYŐI MELINDA	PÉNZÜGYI ÜGYINTÉZŐ	2026.07.08.	Natyelka-Besenyői Melinda
MAGYAR RÓBERT	PÉNZÜGYI ÜGYINTÉZŐ	2026.07.08.	Magyar Róbert
RÉSINDELY MIKLÓSNÉ	PÉNZÜGYI ÜGYINTÉZŐ	2026.07.08.	Résindely Miklósné
TAKÁCS LÍVIA	PÉNZÜGYI ÜGYINTÉZŐ	2026.07.08	
Csiki Zoltán	műszaki ügyintéző	2026.07.08	
LÁDI JÁNOSNÉ	MUNKAÜGYI ÜGYI	2026.07.08	Ládi Jánosné