BDV3089350

Budapest Főváros I. kerület Budavári Polgármesteri Hivatal

Víziváros - Vár - Krisztinaváros - Tabán - Gellérthegy

JEGYZŐ

3/2018. (01.15.) számú Jegyzői Utasítás

Budapest Főváros I. kerület Budavári Polgármesteri Hivatal

Informatikai Biztonsági Szabályzatáról

Budapest Főváros I. kerület
Budavári Polgármesteri Hivatal
Budapest, I. kerület Kapisztrán tér 1
ügyintéző 2018 JÚL 03. előirat
H. P. ......db melléklet
Iktatószám 14692-1/2018

1. A Budapest Főváros I. kerület Budavári Polgármesteri Hivatal Informatikai Biztonsági Szabályzatát az alábbiak szerint adom ki.

2. Jelen Szabályzat rendelkezéseit 2018. január 15-től kell alkalmazni.

Budapest, 2018. január 15.

dr.Herpai-Nagy Teodóra
jegyző

Budapest Főváros I. kerület Budavári Polgármesteri Hivatal, Jegyzői Referatúra
1014 Budapest, Kapisztrán tér 1. * Levélcím: 1250 Budapest, Pf.: 35.
Internet: www.budavar.hu – E-mail: jegyzo@budavar.hu * Fax: 458-3001

BUDAPEST FŐVÁROS I. KERÜLET BUDAVÁRI POLGÁRMESTERI HIVATAL

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT
1.02

BELSŐ HASZNÁLATRA!

2018.

Tartalomjegyzék

- IBSZ DOKUMENTUM VERZIÓ ÉS VÁLTOZÁSKEZELÉS 5
1. A SZABÁLYZAT CÉLJA 6
2. A SZABÁLYZAT HATÁLYA 6
2.1. Személyi hatály 6
2.2. Tárgyi hatálya 7
2.3. Területi hatály 7
3. FELÜLVIZSGÁLAT 7
3.1. Felülvizsgálat 7
4. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE 7
4.1. Informatikus 7
4.2. Az információbiztonság koordinálása és a belső ellenőrzés szerepe 8
4.3. Informatikai biztonsági felelős(IBF) 8
4.4. Adatgazda feladata 10
4.5. Rendszermérnök és Rendszergazda feladatai 10
4.6. A Hivatal szakterületi vezetőinek feladata a szabályzattal összefüggésben 11
4.7. A Hivatal munkatársainak feladata a szabályzattal összefüggésben 11
4.8. Titoktartási megállapodások 12
4.9. A Hivatal biztonsági szintje 12
4.10. Az elektronikus információs rendszerek biztonsági osztályba sorolása 12
5. ÜGYFELEK ÉS EGYÉB SZERZŐDÉSES PARTNEREK 13
5.1. A külső partnerekkel összefüggő informatikai biztonsági kockázatok azonosítása 13
5.2. Az informatikai biztonság az ügyfelekkel való kommunikáció/kapcsolattartás során 13
6. VAGYONTÁRGYAK KEZELÉSE 14
6.1. Vagyonleltár 14
6.1.1. Az adatvagyon leltár 14
6.1.2. Informatikai vagyonleltár 14
6.1.3. Informatikai adatok és rendszerek „tulajdonosa" 14
6.1.4. Informatikai eszközök (adatok és rendszerek) használata 14
6.2. Információk osztályozása 15
6.2.1. Osztályozási elvek 15
6.2.2. Az informatikai eszközök biztonsági szintjeinek meghatározása 15
7. AZ EMBERI ERŐFORRÁSOK BIZTONSÁGA 17
7.1. Az alkalmazást megelőzően 17
7.2. Az alkalmazás időtartama alatt 18
7.3. Az alkalmazás megszűnése, illetve megváltozása 19
7.4. Eljárás a Hivatallal szerződéses viszonyban álló partnerek esetén 19
8. FIZIKAI VÉDELEM ÉS A KÖRNYEZET VÉDELME 19
8.1. Területek védelme, biztosítása 19
8.1.1. Fizikai biztonsági határzóna 19
8.1.2. Fizikai belépés ellenőrzése 20
8.1.3. Külső és környezeti veszélyekkel szembeni védelem 20
8.1.4. Munkavégzés a Szerverszobában (védett terület) 20
8.2. Berendezések védelme 21
8.2.1. Berendezések elhelyezése és védelme 21
8.2.2. Kábelbiztonság 21

8.2.3. Berendezések karbantartása 21
8.2.4. Berendezések biztonsága a telephelyen kívül 22
8.2.5. Berendezések biztonságos selejtezése, illetve újrafelhasználása 22
9. A KOMMUNIKÁCIÓ ÉS AZ ÜZEMELTETÉS IRÁNYÍTÁSA 22
9.1. ÜZEMELTETÉSI ELJÁRÁSOK ÉS FELELŐSSÉGI KÖRÖK 22
9.1.1. Dokumentált üzemeltetési eljárások 22
9.1.2. Változáskezelés 22
Konfiguráció kezelés 23
Változás kezelés menete 23
Sürgősségi változáskezelési eljárás 23
Hibajavítás 23
9.1.3. Az üzemeltetési feladatok, kötelezettségek elhatárolása 23
9.2. HARMADIK FELEK SZOLGÁLTATÁSNYÚJTÁSÁNAK IRÁNYÍTÁSA 23
9.2.1. Szolgáltatásnyújtás 23
9.3. RENDSZERTERVEZÉS- ÉS ELFOGADÁS 24
9.3.1. Rendszerek elfogadása, átvétele 24
9.4. VÉDELEM A ROSSZINDULATÚ ÉS MOBIL KÓDOK ELLEN 24
9.4.1. Rosszindulatú kód elleni intézkedések 24
9.4.2. Mobil kód elleni intézkedések 24
9.5. BIZTONSÁGI MENTÉS 24
9.5.1. Információk biztonsági mentése 24
9.6. HÁLÓZATBIZTONSÁG KEZELÉSE 25
9.6.1. Hálózatok védelme 25
9.6.2. Hálózati szolgáltatások biztonsága 25
9.6.3. Az eltávolítható adathordozók kezelése 25
9.6.4. Adathordozók törlése 25
9.6.5. Adathordozók selejtezése 25
9.6.6. Rendszerdokumentáció védelme 26
9.7. INFORMÁCIÓCSERE 26
9.7.1. Fizikai adathordozók 26
9.7.2. Az elektronikus levelezés biztonsága 26
9.7.3. Okostelefonok használata 28
9.8. ELEKTRONIKUS KERESKEDELMI SZOLGÁLTATÁSOK 28
9.8.1. Nyilvánosan hozzáférhető információk 28
9.9. FIGYELEMMEL KÖVETÉS (MONITORING) 28
9.9.1. Az informatikai rendszer naplózása 28
9.9.2. Órajelek szinkronizálása 30
10. HOZZÁFÉRÉS-ELLENŐRZÉS 30
10.1. FELHASZNÁLÓI HOZZÁFÉRÉS IRÁNYÍTÁSA 30
10.1.1. Felhasználók regisztrálása, felhasználói jelszavak kezelése és ellenőrzése 30
10.2. FELHASZNÁLÓI FELELŐSSÉGEK 30
10.2.1. Jelszóhasználat 30
10.2.2. Őrizetlenül hagyott felhasználói berendezések, tiszta képernyő politika 31
10.3. HÁLÓZATI SZINTŰ HOZZÁFÉRÉS ELLENŐRZÉS 31
10.3.1. Hálózati szolgáltatások használatára vonatkozó szabályzat 31
10.3.2. Hálózathoz való csatlakozás ellenőrzése 31
10.3.3. Külső rendszerekből történő hozzáférés szabályozása 32
11. INFORMÁCIÓS RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS FENNTARTÁSA 32

11.1. INFORMÁCIÓS RENDSZEREK BIZTONSÁGI KÖVETELMÉNYEI 33
11.1.1. Biztonsági követelmények elemzése és meghatározása 33
11.2. HELYES INFORMÁCIÓFELDOLGOZÁS AZ ALKALMAZÁSOKBAN 33
11.2.1. Az adatfeldolgozás ellenőrzése 33
11.2.2. A végfelhasználók által irodai alkalmazásokkal előállított dokumentumok kezelésének irányelvei 33
11.3. RENDSZERFÁJLOK BIZTONSÁGA 33
11.3.1. Üzemelő szoftverek ellenőrzése 33
11.3.2. Programok forráskódjához való hozzáférés ellenőrzése 34
11.4. BIZTONSÁG A FEJLESZTÉSI ÉS TÁMOGATÓ FOLYAMATOKBAN 34
11.4.1. Változás-szabályozási eljárások 34
11.4.2. Alkalmazások műszaki átvizsgálása az üzemelő rendszerek megváltoztatását követően ..35
11.4.3. A rendszer fejlesztési életciklusa 35
11.5. MŰSZAKI SEBEZHETŐSÉG KEZELÉSE 35
11.5.1. A műszaki sebezhetőségek vizsgálata 35
11.5.2. Belső és külső sebezhetőségi vizsgálatok lefolytatása 35
11.6. INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE 36
11.6.1. Információbiztonsági események és gyengeségek jelentése 36
12. MŰKÖDÉS FOLYTONOSSÁGÁNAK IRÁNYÍTÁSA 36
12.1. A MŰKÖDÉS FOLYTONOSSÁGA IRÁNYÍTÁSÁNAK INFORMÁCIÓBIZTONSÁGI SZEMPONTJAI 36
12.2. AZ INFORMÁCIÓBIZTONSÁG A MŰKÖDÉSFOLYTONOSSÁG IRÁNYÍTÁS FOLYAMATÁBAN 36
12.3. AZ INFORMÁCIÓBIZTONSÁGOT MAGUKBAN FOGLALÓ FOLYTONOSSÁGI TERVEK KIDOLGOZÁSA, MEGVALÓSÍTÁSA, TESZTELÉSE 37
12.4. ÜZLETMENET FOLYTONOSSÁGI TERVEK VIZSGÁLATA, FENNTARTÁSA ÉS ÚJRAÉRTÉKELÉSE 37
12.5. RENDSZER KARBANTARTÁSI ELJÁRÁSREND 37
- RENDSZERES KARBANTARTÁS 37
KARBANTARTÁSI NAPLÓ 60
13. JOGSZABÁLYOKNAK ÉS SZABVÁNYOKNAK VALÓ MEGFELELÉS, ÉS MŰSZAKI MEGFELELŐSÉG. 38
13.1. JOGSZABÁLYOK 38
13.2. SZABVÁNYOK 39
13.3. AZ IBSZ-HEZ KAPCSOLÓDÓ BELSŐ SZABÁLYOZÓK ÉS ALKALMAZOTT MÓDSZERTANOK JEGYZÉKE 39
"A" MELLÉKLET - A SZABÁLYZATBAN HASZNÁLT FOGALMAK MEGHATÁROZÁSAI 40
„B" MELLÉKLET - AZ INTERNET HASZNÁLATÁRA VONATKOZÓ BIZTONSÁGI STANDARDOK 51
„C" MELLÉKLET - AZ ELEKTRONIKUS LEVELEZÉSRE VONATKOZÓ BIZTONSÁGI STANDARDOK 52
„D" MELLÉKLET - SZÁMÍTÓGÉPES VÍRUSOKRA VONATKOZÓ BIZTONSÁGI STANDARDOK 53
„E" MELLÉKLET - NYILATKOZAT AZ INFORMATIKAI ESZKÖZÖK ÉS SZOLGÁLTATÁSOK HASZNÁLATÁRÓL 55
- „F" MELLÉKLET- VÁLTOZÁSKEZELÉSI LAP 56
- „G" MELLÉKLET- TITOKTARTÁSI NYILATKOZAT 57
- „H" MELLÉKLET- A ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BESOROLÁSA 58

- **IBSZ dokumentum verzió és változáskezelés**

Verzió	Leírás	Szerző(k)	Lezárás dátuma
1.0	Dokumentum elkészítése		
1. 01	Felülvizsgálat	Hergár Péter	2017.07.08
1.02	Felülvizsgálat	Hergár Péter	2018.01.11

1. A Szabályzat célja

A Budapest Főváros I. kerület Budavári Polgármesteri Hivatala (a továbbiakban: Hivatal) üzleti stratégiájának tervezése és feladatai megvalósításának elősegítése érdekében folyamatait informatikai eszközök használatával teszi hatékonyabbá és gazdaságosabbá. Az informatikai eszközök egyre szélesebb körű használata és az információtechnológia fejlődése azonban új, eddig nem tapasztalt, változó és mindig megújuló kockázatot is jelent a Hivatal számára. Ezt felismerve, az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ vagy Szabályzat) célja egységes keretszabályokat, értelmezéseket, iránymutatást adni az informatikai eszközök üzemeltetői, fejlesztői, felhasználói számára, rögzítve azokat a szabályokat, melyeket a munkakörükhöz rendelt adatok kezelése során követniük kell.

A Szabályzat általános iránymutatással, fogalmi keretrendszerrel és irányelvekkel szolgál az Hivatal által használt informatikai rendszerekben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása és az ezt elősegítő védelmi intézkedések megteremtése érdekében.

A Szabályzat célja továbbá, hogy átlátható és nyomon követhető formában rögzítse azon célokat és irányelveket, amelyek segítségével az információbiztonság magasabb fokú kialakításának további szabályozása, dokumentumai komplex, átfogó és széles körű információbiztonságot alkossanak.

A Szabályzat:

a) meghatározza azokat az alapvető biztonsági normákat és működési kereteket, amelyek érvényesítésével a Hivatal az adatkezelés és adatfeldolgozás kockázatait minimalizálni képes,

b) rögzíti a Hivatal által kezelt adatok feldolgozásával szemben támasztott biztonsági követelményeket,

c) meghatározza az adatbiztonsággal összefüggő szerepeket, felelősség- és jogköröket,

d) elősegíti a számítástechnikai alkalmazások, berendezések, hálózati eszközök biztonságos működését.

e) meghatározza a jogosultság és a hozzáférés rendszerét

f) rögzíti a Hivatal elektronikus információs rendszereinek a jogosultság és hozzáférési szabályozását

2. A Szabályzat hatálya

2.1. Személyi hatály

A Szabályzat személyi hatálya kiterjed

- a Hivatal valamennyi szervezeti egységére,
- a Hivatal minden alkalmazottjára, munkavállalójára,
- a Hivatal egyéb, szerződéses jogviszonyban tevékenykedő partnereire, akik a Hivatal informatikai rendszerével kapcsolatba kerülnek, így különösen: szoftver fejlesztésével vagy módosításával, hardver alkalmazásával és/vagy változtatásával, adatbevitellel és/vagy adatfelhasználással, adatfeldolgozással, hálózat üzemeltetéssel, kapcsolatos tevékenységet végeznek, vagy azzal adat(csere) kapcsolatban állnak, illetve adatfeldolgozásra (is) szolgáló helyszínt üzemeltetnek.

A szabályzat rendelkezéseit érvényre kell juttatni a Hivatal informatikai erőforrásaihoz kapcsolódó fejlesztési feladatokban résztvevő külső partnerekkel kötött szerződésekben, továbbá minden kiszervezési szerződésben, amelyek keretében a szolgáltatónak a vállalt szolgáltatás és/vagy kiszervezés területén meg kell felelnie a jelen utasításban meghatározott feltételeknek és követelményeknek.

2.2. Tárgyi hatálya

A szabályzat tárgyi hatálya kiterjed

a) a Hivatal bármely szervezeti egysége vagy a Hivatallal egyéb jogviszonyban álló személy által munkavégzéssel kapcsolatban használt, illetve a Hivatal adatait feldolgozó, tároló vagy továbbító információhordozó eszközre. Az informatikai eszközök és berendezések (számítógépek, mobil eszközök, nyomtatók, külső adattároló eszközök, aktív hálózati elemek, elektronikus adathordozók stb.) tekintetében minden olyan eszközre, amelyet a Hivatal üzemeltet.

b) a fenti a) pontban meghatározott eszközökre és rendszerekre vonatkozó minden dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési stb. dokumentumok), függetlenül azok formátumától (papír vagy elektronikus),

c) az informatikai eszközökön használt vagy tárolt szoftverekre és adatokra (rendszerprogramok, alkalmazások, adatbázisok stb.), ideértve az üzemelő rendszerek adatain kívül az oktatási, teszt és egyéb célra használt adatokat is,

d) a Hivatal által kezelt és üzemeltetett eszközökön tárolt adatok teljes körére, felmerülésüktől, feldolgozási és tárolási helyüktől függetlenül.

2.3. Területi hatály

Az IBSz területi hatálya kiterjed a Hivatal telephelyére továbbá mindazon objektumokra és helyiségekre, amelyekben az IBSz tárgyi hatálya alatt meghatározott eszközöket, szoftvereket, adatokat vagy dokumentumokat, információkat hoznak létre, tárolnak, használnak vagy továbbítanak.

Nem tartoznak az IBSz területi hatálya alá azon helyiségek, ahol nem kerülnek felhasználásra, illetve nem keletkeznek olyan információk, amelyekben a nyilvánosnál magasabb biztonsági besorolású adatok szerepelnének, valamint a Hivatal azon helyiségei, amelyekben nem üzemeltet informatikai eszközöket, berendezéseket.

3. Felülvizsgálat

3.1. Felülvizsgálat

A Szabályzatot legalább évente felül kell vizsgálni, melynek végrehajtása az informatikai biztonsági felelős feladata.

Amennyiben a Hivatal informatikai biztonságpolitikai helyzetében változás következik be, a szabályzat naprakészségének biztosítása, aktualizálása az informatikus javaslata alapján az informatikai biztonsági felelős feladata.
Jelen szabályzat csak a jegyző engedélyével módosíthatóak, és a „Verziók és változáskezelés" menüpontban és az IBSZ változáskezelési melléklet kitöltésével a módosítás tényét jelezni kell.

4. Az információbiztonság szervezete

4.1. Informatikus

Az informatikus feladata az informatikai folyamatok szerep- és felelősségi köreit kialakítása, az informatikai feladatokat ellátó szerepkör gyakorlóinak számon kérhetőségét megteremtse. (A feladat- és felelősségi köröket az érintett munkatársak munkaköri leírásában a közvetlen szakmai felettes nevesíti.) Az informatikus feladata az alkalmazási rendszerek és az informatikai rendszer biztonságos működtetése feltételeinek biztosítása, illetőleg az ehhez szükséges személyi és tárgyi erőforrás szükséglet jelzése, az információk hozzáférési jogosultság szerinti kezelése feltételeinek a megteremtése.

Az informatikus feladatát képezi továbbá az alkalmazási rendszerek fejlesztése, átvétele és üzemeltetése során az informatikai biztonsági előírások megvalósításáról szóló döntések meghozatala, végrehajtatása és annak vezetői ellenőrzése.

Az informatikus ellátja az informatikai rendszerek üzemeltetésben részt vevő külső, vagy belső munkatársainak irányítását, ellenőrzését, az informatikai hibák kezelésének a figyelemmel kísérését, katasztrófa-elhárítási tervek naprakészen tartásának irányítását, informatikai adathordozók védelmi rendszere kialakításának, végrehajtásának az irányítását, az adathordozók megsemmisítésének az ellenőrzését. Az informatikus részt vesz az informatikai vonatkozású rendkívüli események kivizsgálásában.

Az informatikus gondoskodik az információ védelmi rendszer kialakításáról, fejlesztésének előkészítéséről, illetve döntést követően annak végrehajtásáról, az ahhoz kapcsolódó biztonsági előírások érvényesítéséről. Az informatikus köteles továbbá elkészíteni a fentiekben meghatározott feladatokhoz szükséges informatikai költségvetést.

Az informatikus feladatkörébe tartozik továbbá:

- az informatikai és irodatechnikai eszközök biztonságos és szakszerű működését biztosító kellékanyagok, alkatrészek, kiegészítők beszerzéséért, felhasználásának nyilvántartásáért, időben történő újrarendeléséért,

- a hálózat hardver és szoftver elemeiről folyamatos nyilvántartás készítése,

- a hardver és szoftver nyilvántartás kezelése, változás esetén aktualizálása,

- adatbázis, adatstruktúra dokumentációk kezelése, változás esetén aktualizálása, vagy annak elvégeztetése a szerződéses partnerrel,

- rendszerdokumentációk kezelése, változás esetén aktualizálása, vagy annak elvégeztetése a szerződéses partnerrel,

- A Gazdasági Irodának rendszeres tájékoztatása a tárgyi eszközök leltárkörének esetleges változásairól.

4.2. Az információbiztonság koordinálása és a belső ellenőrzés szerepe

A Hivatal vezetője az információ- és informatikai biztonsági szempontok érvényesülésének ellenőrzése, illetőleg e szempontok érvényesülésének elősegítése érdekében az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11. § (c) pontjával és a 41/2015. (VII. 15.) BM rendelettel összhangban informatikai biztonsági felelőst nevez ki.

4.3. Informatikai biztonsági felelős(IBF)

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 13. § -a alapján az informatikai biztonsági felelős feladatai, jogkörei, és személyi feltételei a következők:

13. §

(1) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

(2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

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

b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,

d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,

e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,

f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

(3) Az elektronikus információs rendszer biztonságáért felelős személy e törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

(4) Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

(5) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését

a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe,

a közreműködők e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

(6) Az elektronikus információs rendszer biztonságáért felelős személy e törvény szerinti feladatai és felelőssége az (5) bekezdés szerinti esetekben más személyre nem átruházható.

(7) Az elektronikus információs rendszer biztonságáért felelős személy jogosult az (5) bekezdés szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

(8) A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.

(9) A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.

(10) Nem kell a (8) bekezdés szerinti képzettséget megszereznie annak a személynek, aki rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.

(11) Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.

Az informatikai biztonsági felelős éves ellenőrzési ütemterv alapján látja el feladatait. Hivatal Elektronikus Információs Rendszereit(EIR) az IBF havi vagy negyedéves rendszerességgel elemzi, igény esetén jelentést készít azokról. Fokozott kockázatra utaló jelek észlelése esetén javaslatokkal él.

Az informatikai biztonsági felelős által ellátott – alapvetően a Hivatal informatikai eszközeinek fizikai és logikai biztonságát célzó – feladatok körében szakmailag a belső ellenőrzés irányítása alá tartozik. Az informatikai biztonsági felelős szakmailag a belső ellenőrzés irányítása alá tartozik, de feladatait önállóan, a szakmai követelmények betartása mellett látja el. Tapasztalatairól, jelentéseiről az első számú vezető, és az informatikus mellett folyamatosan tájékoztatja a belső ellenőrt is. A belső ellenőr által végzett informatikai vizsgálatokba az informatikai biztonsági felelős bevonható, kivéve azon területet, mely az informatikai biztonsági felelős tevékenységének ellenőrzésére irányulnak.

4.4. Adatgazda feladata

A Hivatal valamennyi funkcionális területének vezetője köteles egy személyt kirendelni a funkcionális területen használt adatok gazdájául. A továbbiakban az adatgazda lesz felelősségre vonható az illető terület adatainak az adatbiztonsági előírásokban megfogalmazottak szerinti kezeléséért. Indokolt esetben az adat gazdája a funkciójából fakadó napi kötelezettségeit, hatáskörét átruházhatja más személyre vagy személyekre. Az adatgazda azonban ettől az átruházástól függetlenül a továbbiakban is felel a kérdéses adat vagy adatok biztonságáért.

Kötelességei

- Meg kell határoznia valamennyi, a saját funkcionális területén belül használt adatot.
- Osztályoznia kell a saját funkcionális területén belül használt adatokat a hozzájuk kapcsolódó bizalmasan történő kezelés, sértetlenség és hozzáférhetőség iránti igény szintje szerint és erről nyilvántartást kell vezetnie.
- Gondoskodik a hozzáférési rendszer (információs rendszerekben definiált szerepkörök és elemi jogosultságok) meghatározásáról és karbantartásáról.
- Gondoskodnia kell arról, hogy az adatok elérhetőségét figyelembe vegyék az üzletmenet folyamatosságának fenntartására és az üzemszerű működés helyreállítására vonatkozó tervekben.
- Abban az esetben, ha harmadik félnek adnak át a Hivatal üzleti titkának minősülő adatokat, fel kell mérnie az átadással járó veszélyt, s annak nagyságától függően meg kell határoznia a megfelelő megelőző óvintézkedéseket – még az adatok átadása előtt (pl. Titoktartási nyilatkozat aláíratása a harmadik féllel).
- Döntést kell hozni és jóváhagyást kell adni arról, hogy kinek legyen hozzáférési joga az adott üzletági területen használt adatokhoz és az azokhoz történő hozzáférést biztosító számítástechnikai információs rendszerekhez.
- Biztosítania kell, hogy az adatbiztonsági szabályok esetleges megszegése esetén megtörténjen az elkövetett szabálysértés körülményeinek feltárása és a jelentés megtétele.

4.5. Rendszermérnök és Rendszergazda feladatai

A Hivatal számára a rendszergazdai és rendszermérnöki feladatokat kiszervezési szerződés keretében külső szolgáltató látja el.

A cégvezetés által definiált követelményrendszernek megfelelően, jelen szabályzat és a szakmai előírások figyelembevételével a rendszergazda biztosítja az informatikai rendszer folyamatos, üzemszerű és biztonságos működését.

Kötelességei közé tartozik különösen:

- a hálózat szervereinek üzemben tartása,

- a szerverek indítása, leállítása, diagnosztikája, az időszakos mentések elvégzése,

- a rendszer hardware elemekkel való bővítése, ill. szűkítése, munkaállomások felkészítése a hálózati működésre,

- az felhasználói fiókok kezelése; új felhasználók, ill. felhasználói csoportok létrehozása és a már létezők megszüntetése,

-elektronikus levelezési fiók beállítása

A rendszermérnök biztosítja az informatikai rendszerek biztonságos konfigurálását:

- a hálózat konfigurálása, hálózati kapcsolatok létrehozása, karbantartása, ellenőrzése,

-határvédelmi eszközök konfigurációja, karbantartása

- a nyomtatók integrálása a hálózatba.

- a hálózati hozzáférési jogok (Active Directory) beállítása, karbantartása, a megfelelő könyvtár-struktúra kialakítása, felhasználói programok területének kijelölése, a felhasználók munkaterületének beállítása,

- Napi, időszakos és rendszermentések megszervezése elvégzése, a mentési szabályzatban leírt módon

- *466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról* kapcsolatos archiválási feladatok végrehajtása

4.6. A Hivatal szakterületi vezetőinek feladata a szabályzattal összefüggésben

Minden üzleti és funkcionális terület vezetője köteles a Szabályzat betartásáról és betartatásáról gondoskodni, és a Szabályzat előírásait megszegőkkel szemben következetesen fellépni.

4.7. A Hivatal munkatársainak feladata a szabályzattal összefüggésben

A Hivatal minden munkatársa köteles a Szabályzatot megismerni, a gyakorlati elsajátítását elősegítő oktatáson részt venni, és a munkaköri feladatainak ellátása során a Szabályzat előírásait megtartani. Aki a Szabályzat előírásainak megsértését, a számítástechnikai erőforrásokkal történő visszaélést, kárt vagy kockázatot okozó magatartást (tevékenységet vagy mulasztást), vagy mindezek veszélyét tapasztalja, köteles azt a közvetlen szakmai felettesének, és az informatikusnak késedelem nélkül jelenteni.

A Hivatal valamennyi munkavállalója csak a munkakörébe tartozó feladatok maradéktalan és hatékony ellátása által indokolt körben kaphat hozzáférést a Hivatal informatikai rendszereihez és az azokban nyilvántartott és/vagy feldolgozott adatokhoz, beleértve a hálózati meghajtók könyvtáraihoz és a könyvtársak adataihoz való hozzáférést is. A hozzáférési jogosultságok megadása, felülvizsgálata és indokolt esetben azok módosítása az adatgazda feladata és felelőssége.

A Hivatal felhasználóinak a felhasználói jogosultságok megadását megelőzően, az ideiglenes szerződéssel rendelkező munkatársak esetében pedig a szerződés aláírásával egyidejűleg alá kell írniuk egy nyilatkozatot („E" melléklet), melyben kijelentik, hogy az:

- informatikai biztonsági szabályzatban,
- Iratkezelési szabályzatban,

foglaltakat elolvasták, azt tudomásul veszik, és betartják. A nyilatkozat tárolása a Hozzáférési jogosultság átvételével együtt történik.

Kötelességei:

- Minden felhasználó köteles megismerni és betartani jelen szabályzatban és az Iratkezelési Szabályzatban rögzített előírásokat a zavartalan és biztonságos működés érdekében,
- Az általa használt eszköz (hardver és szoftver) rendeltetésszerű használatára vonatkozó előírások, használati utasítások betartása,
- Az általa használt eszközök állagmegóvása
- Működési hiba esetén értesíti az informatikust, aki intézkedik a javításról.

Tilos:

- más személyi azonosítóit (felhasználói név, IP cím, bankkártyaszám stb.) használni,
- a hálózat üzemeltetéséhez szükséges szoftver vagy hardver eszközökben kárt tenni,
- szerzői jogokat sértő, valamint jogszabályba ütköző anyagokat terjeszteni,

- a hálózati számítógép, vagy külső számítógépek működését megzavarni, azokra behatolást megkísérelni,
- olyan tevékenység folytatása, amelynek célja vagy előrelátható következménye a hálózati infrastruktúra hardver- vagy szoftverintegritásának sérülése,
- nem engedélyezett erőforrások illetéktelen megszerzése,
- a hálózatban olyan adatok továbbítása, amelyben bármelyik, a feladó azonosítására szolgáló információ hamis. Ide értve: elektronikus levél hamis feladóval történő küldését.
- Számítógépes zaklatás (durva szövegű levelek, fenyegető üzenetek, spam)
- Mások munkájának akadályozása
- Jogosult személyek megakadályozása jogos tevékenységükben
- Hordozható adattárolók, adathordozók, adatok engedély nélküli kivitele

4.8. Titoktartási megállapodások

Minden munkatársnak titoktartási nyilatkozatot kell aláírnia, melyben nyilatkozik, hogy a munkája során tudomására jutott, a Hivatal számára értéket jelentő információt sem a munkavégzése, sem annak vége után sem hozza harmadik fél tudomására.

A Hivatal számára valamely szolgáltatást nyújtó szerződéses partner csak a szerződésszerű teljesítéshez elengedhetetlenül szükséges mértékben és ideig, titoktartási nyilatkozat megtételét követően és megfelelő jogosultság birtokában férhet hozzá a Hivatal érintett informatikai rendszereihez, és azokban nyilvántartott és/vagy feldolgozott adatokhoz. Az ilyen szerződések tervezett tartalmáról a belső adatvédelmi felelőst és az informatikust előzetesen tájékoztatni kell.

Titoktartási nyilatkozat az IBSZ „G" melléklete.

4.9. A Hivatal biztonsági szintje

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről 2.1.5 pontja alapján a Hivatal biztonsági szintje 3as.
„Az érintett szervezet biztonsági szintje 3., ha a szervezet vagy szervezeti egység a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe."

4.10. Az elektronikus információs rendszerek biztonsági osztályba sorolása

A 2013. évi L. törvény előírja a Hivatal elektronikus információs rendszereinek kockázatelemzésen alapuló ötfokozatú skálán való biztonsági osztályba sorolását a jogszabályok szerint, valamint nemzetközi szabványok és legjobb gyakorlatok figyelembe vételével. A 2014. 06. 30-án elvégzett biztonsági osztályba sorolás eredményét jelen ***IBSZ „H" melléklete rögzíti***, a kockázatelemzések eredményét és az egyes rendszerekre vonatkozó megfelelést pedig külön dokumentumok tartalmazzák.
A biztonsági osztályba általános szabályai:
a) A biztonsági osztályba sorolás eredményét a szervezet vezetője hagyja jóvá és felel annak jogszabályoknak megfelelő, jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért.
b) A biztonsági osztályba sorolás eredményét minden esetben az Informatikai Biztonsági Szabályzatban, vagy annak mellékletében rögzíteni kell és védeni kell a jogosulatlan megismeréstől.
c) A biztonsági osztályba sorolás eredményét három évente, valamint minden olyan esetben dokumentálható módon felül kell vizsgálni, amikor azt a szervezet, a jogszabályi környezet,

a személyi állomány vagy a technológiai környezet változása megköveteli.
d) Soron kívül el kell végezni a biztonsági osztályba sorolást új elektronikus információs rendszer bevezetésekor.
e) Amennyiben a biztonsági osztályba sorolás során a Hivatal hiányosságot állapít meg 90 napon belül cselekvési tervet kell készíteni a szükséges védelmi intézkedések

megvalósítása érdekében.

5. Ügyfelek és egyéb szerződéses partnerek

5.1. A külső partnerekkel összefüggő informatikai biztonsági kockázatok azonosítása

A Hivatal külső partnere lehet:

a) kiszervezett tevékenységet ellátó személy,

b) egyéb szerződéses partner.

A kiszervezett tevékenységet végzővel szemben támasztott informatikai biztonsági követelmények nem lehetnek enyhébbek, mint a Hivatallal szemben támasztott jogszabályi követelmények.
A kiszervezési szerződéseknek a kiszervezett tevékenységet végző tudomására jutott adatok jellege és azok minősítése által indokolt terjedelemben konkrétan tartalmazniuk kell a kiszervezett tevékenységet végzővel szemben támasztott követelményeket, és azok megvalósulása érdekében teendő intézkedéseket.

A Hivatal jogi referense – az informatikai biztonsági követelmények szempontjából – minden esetben felülvizsgálja a Hivatal külső partnerekkel kötött – nem csak kiszervezésnek minősíthető – szerződéseit. Az általa tett észrevételeket megvitatja az érintett szakterületi vezetőkkel, valamint az informatikussal.

5.2. Az informatikai biztonság az ügyfelekkel való kommunikáció/kapcsolattartás során

A Hivatal az ügyfelei számára az alábbi módokat biztosítja a kapcsolattartásra:

a) E-mail

b) Internetes weboldal

c) Telefon

Az ügyfél adatainak kezelése, továbbá kezelt adataik tekintetében az ügyfeleket megillető jogosultságok érvényesülésének biztosítása mindenkor az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseinek megfelelően történhet.

5.3. A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

Amennyiben a Hivatal szerződésbe lép olyan külsős partnerrel, aki a Hivatal informatikai rendszerével kapcsolatba kerül, így különösen: szoftver fejlesztésével vagy módosításával, hardver alkalmazásával és/vagy változtatásával, adatbevitellel és/vagy adatfelhasználással, adatfeldolgozással, hálózat üzemeltetéssel, kapcsolatos tevékenységet végez, vagy azzal adat(csere) kapcsolatban áll, illetve adatfeldolgozásra (is) szolgáló helyszínt üzemeltet, akkor a Hivatal:
a) Az Informatikai biztonsági szabályzat előírásai alapján meghatározza a külső szervezet munkatársaira vonatkozó biztonsági követelményeket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is,
b) Szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg a Hivatal által meghatározott, külső szervezetek munkatársaira vonatkozó biztonsági követelményeknek,
c) Dokumentálja a külső szervezetek munkatársaira vonatkozó biztonsági követelményeket,
d) Előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az Hivatal elektronikus információs rendszeréhez kapcsolódó felhasználói azonosítóval, hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek,
e) Fenntartja magának a jogot, hogy ellenőrizhesse, és rendszeresen ellenőrzi is azt, hogy a szerződő

fél megfelel-e a munkatársaira vonatkozó biztonsági követelményeknek.

6. Vagyontárgyak kezelése

6.1. Vagyonleltár

6.1.1. Az adatvagyon leltár

Üzleti folyamataink alapja az információ (értelemmel bíró adat). Sérülése, elvesztése, esetleges ellopása anyagi károkat okozhat, nem beszélve a működési és reputációs következményekről. Ezeknek a kockázatoknak a minimalizálása érdekében ismernünk kell az adataink előfordulási helyét és felhasználásának sajátosságait. Az adatvagyon felmérés lajstromba veszi az üzleti folyamatokhoz kapcsolódó lényeges adatokat.

A védelem szervezéshez elengedhetetlen az adatvagyon struktúrájának, értékének, az egyes adatok üzleti folyamatokhoz való kapcsolódásának feltárása, mert a védelem szükséges szintje ezeknek a tényezőknek az összességéből következik. Nem jelentéktelen a biztonságszervezés szempontjából az sem, hogy ténylegesen mi az, amit védeni szeretnénk, hol és milyen formában tároljuk. Az adatvagyon leltár egyben segítség a feleslegesen tárolt és feldolgozott adatok mennyiségi megismerésében, ezen ismeret birtokában a racionális intézkedések meghozatalában, és nem utolsó sorban a felhasználók adatvédelmi attitűdjének jobbításában is.

Adatvagyon leltár egy eredménytermék, amely alapja nem csak a hatékony informatikai és információbiztonsági szabályozásoknak, de az adatgazdák kijelölésének is.

6.1.2. Informatikai vagyonleltár

Az informatikai vagyongazdálkodás, a teljes körű hardver- és szoftver leltár, amellett, hogy naprakésszé és átláthatóvá teszi a Hivatal informatikai eszközeinek és licenceinek kezelését, segíti az ezekhez tartozó igénylési, nyilvántartási és beszerzési folyamat racionalizálását.

Az IT leltár ugyanakkor hasznos eszköz a projektetek tervezésekor, előkészítésekor, mert a leltáradatok segítenek megbecsülni a várható költségeket, kockázatokat, de egyben jól használható kontrolleszköz a projektek megvalósulásának ellenőrzésekor is.

A Hivatal hardver és szoftver leltárának naprakész és átlátható vezetésének ellenőrzése az informatikus feladata.

A szoftver leltár tartalmazza:

- Szoftver neve
- Forgalmazó (a számlán szereplővel megegyező módon)
- Verziószám
- Szoftver jogtulajdonos
- Tulajdonba kerülés dátuma
- Példányszám

A Hivatal tulajdonában lévő, aktivált számítástechnikai eszközökről az általános leltári szabályoknak megfelelően leltárt kell készíteni.

A leltározást végző személyeket, annak időpontját és időtartamát a pénzügyi igazgató határozza meg. Az egyes eszközök nyilvántartásba vételekor az eszközökre leltári azonosító szám kerül. Számítógépbe vagy egyéb helyre (pl.: HUB bővítés) történő, számítástechnikai eszközépítést a beépítési hely leltári kartonjára át kell vezetni. A leltári kartotékokat a Gazdasági Iroda kezeli.

Épületen belüli számítástechnikai eszközmozgást a Gazdasági Iroda tudomására kell hozni (melyik szobából, melyik szobába, mikor, ki rendelte el az áthelyezést).

6.1.3. Informatikai adatok és rendszerek „tulajdonosa"

Az aljegyző a Hivatal vezetésével együttesen kidolgozott eljárás keretében jelöli ki hivatalosan a Hivatal Elektronikus Információs Rendszereinek(EIR) tulajdonosát, azaz az adatgazdát, aki dönt az adatok osztályozásáról és a hozzáférési jogosultsági szintekről. A Hivatal besorolásait az IBSZ „H" melléklete tartalmazza.

6.1.4. Informatikai eszközök (adatok és rendszerek) használata

A felhasználók azonosítását és hozzáférési jogait – amennyiben nincs egyedi azonosítás a rendszerek és az adatgazdák azonosítását egyetlen központi rendszerben kell kezelni, a hozzáférési jogosultság ellenőrzés hatékony és egységes megvalósítása érdekében.

Az informatikai eszközök elfogadható használatához tartozik, hogy a jogosultság engedélyeken szerepelnie kell az engedélyező aláírásának, továbbá az engedélyezett jognak. A jogosultságokat a leendő felhasználó vezetője kezdeményezi a Jogosultság Igényló Lap(JIL) kitöltésével. A lap megtalálható a közös fájl szerveren.

A jogosultság nyilvántartó rendszerben valamennyi felhasználó minden hozzáférési jogának szerepelnie kell, és a nyilvántartott, valamint az engedélyekben szereplő adatoknak összhangban kell állniuk.

6.2. Információk osztályozása

6.2.1. Osztályozási elvek

A Hivatal teljes feldolgozási-, és végrehajtási munkafolyamataira biztosítani kell a három alapfenyegetettség bekövetkezési valószínűségének csökkentését, vagyis az adatok, információk és az azokat kezelő rendszerek:

a) bizalmasságát,

b) sértetlenségét,

c) rendelkezésre állását.

A bizalmasság annak biztosítása, hogy az információ csak az arra felhatalmazottak számára elérhető. A bizalmasság védelme a felfedés elleni védekezést jelenti.

A sértetlenség azt jelenti, hogy valami az eredeti állapotának megfelel, és a forrása is eredeti. A sértetlenség (integritás) védelme a jogosulatlan változtatás elleni védelmet jelenti, célja az információk és feldolgozási módszerek teljességének és pontosságának megőrzése.

A rendelkezésre állás az erőforrások olyan állapota, amelyben eredeti rendeltetésének megfelelő szolgáltatásokat nyújtani tudja (működőképesség), meghatározott helyen és időben (elérhetőség). A rendelkezésre állás annak biztosítása, hogy a felhatalmazott felhasználók mindig hozzáférjenek az információkhoz, amikor szükséges. A rendelkezésre állás védelme ennél fogva az erőforrások szolgáltatási folyamatosságának védelmét jelenti.

Ezeknek az osztályozási elveknek az alapján kell az adatokat osztályozni, amelyből a védelmi követelmények meghatározhatók.

Az osztályozás arra ad választ, hogy mit és mennyire kell megvédeni. Az informatikai biztonság pedig azt határozza meg, hogy az adatvédelmi osztályozásra tekintettel az informatikai erőforrásokat (így az adatokat is) hogyan kell megvédeni.

Az informatikai vagyon minden elemét be kell sorolni valamelyik szintre, annak megfelelően, hogy működésének megszűnése, vagy az adatok bizalmasságának sérülése hogyan hat a Hivatalra. Az adatgazdák feladata az adatvagyon besorolása, és ezt követően az üzemeltetést ellátó szolgáltató, valamint az informatikus feladata az informatikai alkalmazások és eszközök nyilvántartása. Az adatgazdáknak az általuk felügyelt adatvagyonról nyilvántartást kell vezetni oly módon, hogy az áttekinthető legyen.

6.2.2. Az informatikai eszközök biztonsági szintjeinek meghatározása

A Hivatal informatikai eszközei, valamint a rajtuk futtatott alkalmazásai különböző jelentőséggel bírnak a Hivatal biztonságos működésének szempontjából. Az informatikai eszközök biztonsági szintjét a Hivatal informatikai kockázatelemzésében kell meghatározni, melyről az aljegyző dönt. Az informatikai eszközök biztonsági szintjéről és azok változásairól az informatikusnak kell nyilvántartást vezetni.

A tevékenységek biztonsági kockázatának figyelembe vételével a következő szinteket kell kialakítani.

I. szint:

Az ide tartozó informatikai eszközök, alkalmazások működésének teljes megszűnése elviselhető a Hivatal számára, illetve az adatok bizalmasságának, sértetlenségének az elvesztése jelentéktelen kárt okoz a szervezet számára.

II. szint:

Az ide tartozó informatikai eszközök, alkalmazások működésének hosszabb idejű (1-2 hét) megszűnése elviselhető a Hivatal számára, illetve az adatok bizalmasságának, sértetlenségének az elvesztése csekély kárt okoz a szervezet számára.

III. szint:

Az ide tartozó informatikai eszközök, alkalmazások működésének közepes ideig (3-7 nap) tartó megszűnése elviselhető a Hivatal számára, illetve az adatok bizalmasságának, sértetlenségének az elvesztése közepes kárt okoz a szervezet számára.

IV. szint:

Az ide tartozó informatikai eszközök, alkalmazások rövid távúnál nem hosszabb kiesése (2-3 nap) még elviselhető terheket ró a Hivatalra, illetve az adatok bizalmasságának, sértetlenségének az elvesztése nagy kárt okoz a szervezet számára.

V. szint:

Ide tartoznak az alapfunkciók működtetése és biztonsága szempontjából legfontosabb alkalmazások, rendszerszoftverek, eszközök, berendezések és a környezeti infrastruktúra vonatkozó elemei. Ezen rendszerelemek rövid idejű kiesése (1 nap) , vagy az adatok bizalmasságának vagy sértetlenségének az elvesztése kiemelkedően nagy kárt (katasztrófa) okoz a szervezet számára.

6.2.3. Az adatok osztályozása

Az adatok osztályozását az adatgazdák – a belső adatvédelmi felelőssel egyeztetve- látják el. Ha „személyes adat", „különleges személyes adat" minősítésű adatot tartalmazó dokumentum harmadik fél részére átadásra kerül, erről az adatgazda minden esetben köteles a jogi referenst és belső adatvédelmi felelőst előzetesen értesíteni. Az előzetes értesítés azért szükséges, mert az információs önrendelkezési jogról szóló törvény értelmében az ilyen adatátadásokról (adattovábbításokról) adattovábbítási nyilvántartást kell vezetni. E nyilvántartást a informatikai szolgáltatás manager . Az erre vonatkozó részletes szabályokat az „Iratkezelési szabályzat" címmel kibocsátott – mindenkor hatályos – utasítás tartalmazza.

„Belső használatú adat" megjelölésű adat vagy dokumentum harmadik személy részére történő átadásához a belső adatvédelmi felelős előzetes értesítése nem szükséges. Ugyanakkor az ilyen dokumentum, például egy a Hivatal valamely munkaszervezeti egysége által adott állásfoglalás, személyes adatot (név, telefonszám) nem tartalmazhat.

A Hivatal adatvagyonát osztályozni kell az alábbiak szerint:

Megnevezés	Leírás
Nyilvános adat	A Hivatal tudtával és engedélyével nyilvánosságra hozható adatok köre (honlapon elhelyezett adatok, sajtóközlemények, stb.) továbbá meghatározott természetes személyek azon személyes adatai is, amelyek nyilvánosságát közérdekből jogszabály rendeli el. köztiszvis
Belső használatú adat	A munkavégzés során keletkező olyan adatok, melyek nem tartoznak más, itt felsorolt osztályba, de nem számítanak nyilvánosnak

Megnevezés	Leírás
Üzleti titok	A Polgári Törvénykönyvben meghatározott fogalom *(A gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a szervezet jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, és amelynek titokban tartása érdekében társaságunk a szükséges intézkedéseket megtette.)*
Személyes adat	Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben meghatározott fogalom *(Az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés)*
Különleges adat	Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben meghatározott fogalom *(A faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat)*
Közérdekű adat	Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben meghatározott fogalom *(az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat)*
Közérdekből nyilvános adat	Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben meghatározott fogalom *(a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli)*

7. Az emberi erőforrások biztonsága

A biztonsági kockázatok közül a legnagyobb sebezhetőséget jelentős mértékben a humán kockázatok jelentik. Humán biztonsági kockázatot jelent a megbízhatatlan, elégedetlen munkatárs, de az alapvető informatikai ismeretekkel nem rendelkező köztisztviselő is. Biztonsági szempontból el kell kerülni, hogy nem megbízható munkatársak felvételre kerüljenek, az alkalmazás időtartama alatt pedig fel kell tudni fedni, ha valamely munkatárs megbízhatatlanná válik.

7.1. Az alkalmazást megelőzően

Alapkövetelmények új munkatárs felvételekor:

- 90 napnál nem régebbi hatósági bizonyítvány, amely igazolja, hogy nem szerepel a bűntettesek nyilvántartásában (adott esetben a 2009. évi XLVII. törvény alapján a jelölttől meghatározott bűncselekmények tekintetében is kérhető a büntetlenség igazolása, és/vagy az is, hogy nem áll büntető eljárás alatt),
- szakmai képesítéseket igazoló dokumentumok beszerzése,
- ellenőrizhető referenciák,
- próbaidő kikötése (ettől a munkáltatói jogkör gyakorlójának engedélyével lehet eltérni)
- lehetőség szerint korlátozott jogosultságok
- a KTTV-nek megfelelő hivatkozási pontok.

7.2. Az alkalmazás időtartama alatt

A biztonságos munkavégzés feltételeinek biztosítása, továbbá a munkakör ellátásához szükséges eszközök megteremtése a munkáltató feladata ugyan, a napi munkavégzés során azonban a munkatárs közvetlen szakmai felettese az, aki az új munkatárs próbaideje alatt a tevékenységet folyamatosan monitorozni köteles.

A Hivatal informatikai rendszerének minden belső felhasználóját informatikai biztonsági oktatásban kell részesíteni. A Hivatal vezetése biztosítja az oktatások előfeltételeit, az oktatásokkal kapcsolatos dokumentumok előállítását, tanfolyamok megrendezését, továbbá a szakmai továbbképzés lehetőségét.

Az informatikai biztonsági oktatást meghatározott időközönként – akár belső erőforrás, akár külső szakértő vagy az informatikai biztonsági felelős bevonásával – el kell végezni.

Az oktatási anyagok szakmai tartalmának összeállításáról, naprakészségének és minden felhasználó részére való hozzáférhetőségének biztosításáról, és az oktatások megszervezéséről az informatikus köteles gondoskodni.

Az oktatáson ki kell térni, különösen

a) a felhasználói tudatosság jelentőségére, és az ezzel összefüggésben valamennyi felhasználó felelősségére,

b) az IBSZ főbb rendelkezéseire

c) azoknak a sebezhetőségeknek az ismertetésére, amelyek a felhasználó adat és rendszer biztonságát veszélyeztető magatartását használják ki,

Minden új felhasználó számára a munkába lépést követő egy héten belül biztosítani kell az oktatási anyag megismerhetőségét. A felhasználó az oktatáson való részvételét jegyzőkönyvben aláírásával köteles hitelesíteni. A biztonsági oktatások megtörténtét dokumentálni kell, a jelenlevők névsorával együtt. Az oktatások megtörténtének ellenőrzése az informatikus feladata.

Az informatikai biztonsággal kapcsolatos kockázatokat csökkenti, ha a Hivatal munkavállalói tisztában ismerik a munkafolyamataikat támogató informatikai rendszereket. Az informatikus és a vezető beosztású munkatársak kötelesek személyes magatartásukkal is erősíteni az informatikai biztonsági tudatosságot.

Soron kívüli oktatást kell tartani az érintett munkavállalóknak hardver- és szoftver-eszközök, valamint a használatukat szabályozó eljárások jelentős változásakor. Az ilyen oktatások megtörténtét is *„Jelenléti ív"* alkalmazásával kell dokumentálni.

Az informatikai biztonságot sértő vagy azt veszélyeztető magatartás (tevékenység vagy mulasztás) esetén az informatikai biztonsági felelős vizsgálati eljárást indít, amelynek megállapításait vizsgálati jelentésben rögzíti.

A jelentésnek tartalmaznia kell:

a) magát a biztonságsértést megvalósító magatartást, és annak időpontját

b) a magatartást elkövető munkatárs megnevezését,

c) a biztonsági esemény megvalósítását lehetővé tévő gyengeségek felsorolását,

d) a magatartás következményeit,

e) a magatartás következményeinek megszüntetésére javasolt intézkedéseket,

f) hasonló vagy azonos magatartás megelőzésére javasolt intézkedéseket.

A biztonsági esemény kivizsgálása során az eseménnyel kapcsolatban érintett munkatársaknak együtt kell működniük az informatikai biztonsági felelőssel.

7.3. Az alkalmazás megszűnése, illetve megváltozása

A felhasználói jogosultságok törlése a munkavállaló munkában töltött utolsó napján kell végrehajtani. A munkavállaló szervezeti vezetője köteles az informatikus részére a távozás tényét és napját előzetesen bejelenteni. Ezen alkalommal a szervezeti vezető rendelkezik a távozó munkavállaló adatainak – min. levelezés, fájlban tárolt adatok- hozzáféréséről, archiválásáról rendelkezni.

Amennyiben a munkatárs munkaszerződése a munkakörét érintően módosul, a módosított munkaköri feladatainak ellátáshoz szükséges jogosultságok megadására (beállítására) vagy meghatározott jogosultságok törlésére, ideértve a megszűnt munkakörhöz tartozó jogosultságok törlését is, a jelen szabályzat -10.1. pontjai alapján kitöltött Jogosultság Igénylő Lap kitöltése- az irányadók.

A munkatárs munkaviszonyának megszűnése esetén a munkatárs a használatában lévő számítástechnikai eszközöket köteles visszaszolgáltatni. A számítástechnikai eszközök átadás-átvételének dokumentálása, ideértve az esetleges hiány feltüntetését is, a munkatárs kilépő lapján történik.

7.4. Eljárás a Hivatallal szerződéses viszonyban álló partnerek esetén

A Hivatal számára valamely informatikai, vagy más, az üzletmenet körébe eső, szolgáltatást nyújtó szerződéses partner számára az informatikai erőforrásokhoz való hozzáférés engedélyezése, ellenőrzése, és megszüntetése során a jelen utasítás rendelkezései mellett, a jelen szabályzat 10.1.-ban részletezett utasításokat alkalmazzuk, az informatikai területet érintően a jelszavakat az informatikus kezeli.

8. Fizikai védelem és a környezet védelme

8.1. Területek védelme, biztosítása

8.1.1. Fizikai biztonsági határzóna

A biztonsági követelményeknek megfelelő védelem megteremtéséhez szükséges a fizikai védelem peremsávjának kijelölése, a védendő területek határainak meghatározása. A határok biztosítására kockázatarányos védelmet kell kiépíteni.

a) A fizikai védelem peremsávja a Hivatal telephelyeinek vagy különálló épületeinek határa.

b) A kijelölt peremsávot meg kell erősíteni Portaszolgálattal, riasztóval, CCTV, kamerákkal

c) Recepciót kell kialakítani az érkező látogatók fogadására. A telephelyen és/vagy az épületekben csak arra felhatalmazott személy tartózkodhat.

d) Álpadló és álmennyezet esetén is biztosítani kell a valódi padló és valódi mennyezet közötti fizikai védelmet. Meg kell akadályozni, hogy illetéktelenek lépjenek a helységbe. Tűzjelző berendezést kell felszerelni.

A Hivatal székhelyén lévő, valamint a Hivatal katasztrófa-helyszínén lévő **szerverekre vonatkozóan** az alábbi rendelkezéseket kell betartani:

e) A szerverek zárható helyiségben, gépteremben vannak elhelyezve és üzemeltetve,

f) A szerverszobának kártyás beléptetővel rendelkezik, és biztosítva van a szerverszobába belépő személyek egyedi azonosítása, valamint a be- és jogosults naplózva van.

g) A helyiségbe (szerverszoba, katasztrófa-helyszín) csak jogosultsággal, ennek hiányában csak az

informatikus kíséretében lehet belépni, és ott tartózkodni. A szerverszobában, katasztrófa-helyszínen a mentések tárolására használt, vagy minősített adatokat tartalmazó adathordozókhoz való hozzáférés jogosultság hiányában csak az informatikus kíséretében megengedett.

Az előírások betartását, ideértve a naplózásra vonatkozó követelmények érvényesülését is, az informatikai biztonsági felelős is jogosult ellenőrizni.

8.1.2. Fizikai belépés ellenőrzése

A szerverszoba kialakításánál a következő minimális követelményeknek kell eleget tenni:

a) A szervereknek egyenletes hőmérsékletet és páratartalmat kell biztosítani. Behatolás-védelmi szempontok és „vis major" helyzetek számbavételével a lehető legbiztonságosabb területre van telepíve a szerverszoba.

b) Az informatikai eszközök védve vannak az áramellátás zavaraiból, megszakadásából származó meghibásodás, és/vagy hibás működés ellen.

c) A folyamatos áramellátást biztosítása szünetmentes tápegységek alkalmazásával valósul meg.

d) Minden épületet teljes körű villámvédelemmel kell ellátni. Lehetőség szerint a külső kommunikációs vonalakat is védeni kell villámcsapás ellen.

e) Az áramellátást biztosító szünetmentes tápegységeket (áramforrásokat) rendszeresen ellenőrizni kell. Az ellenőrzések elvégzéséért az informatikus felelős. Az ellenőrzési periódusok meghatározásánál figyelembe kell venni az UPS akkumulátorának korát és gyártó által meghatározott élettartamát.

Az elektromos hálózatban fellépő rendellenességek ellen a szerverszobában megfelelő védelmet kell kialakítani (villámvédelem, feszültség-ingadozás, feszültség csúcsok stb.). Az informatikus köteles monitorozni a szerverszoba és a szerverpark környezeti paramétereit (hőmérséklet, páratartalom, energiaellátás, az ezeket biztosító berendezések (klíma, szünetmentes tápegység) üzemképessége). Meghibásodás veszélye esetén a rendszergazdák kötelesek a szükséges megelőző, elhárító intézkedéseket kezdeményezni, meghibásodás esetén a javítás iránt késedelem nélkül intézkedni, és szükség esetén az informatikai berendezéseket leállítani.

8.1.3. Külső és környezeti veszélyekkel szembeni védelem

Az épületen belül a tűzrendészeti szabályok betartása egységesen vonatkozik minden, az épületben tartózkodó személyre. Az épületen belül a dohányzás nem megengedett. Dohányozni csak az e célra kijelölt helyen szabad. Az épület kijelölt pontjain kötelező tűzoltó palackokat elhelyezni. Csak az ellenőrzéseken átesett, érvényes, jegyzőkönyvezett készülékek használhatóak.
A szerverszobát tűzérzékelő berendezéssel kell felszerelni, mely a diszpécser szolgálaton riaszt.
A szerverszoba beázás elleni védettségét ellenőrizni szükséges, amelyet dokumentálni kell.

8.1.4. Munkavégzés a Szerverszobában (védett terület)

A védett területeken történő munkavégzésre további biztonsági szabályok vonatkoznak.

a) Fokozottan kell érvényesíteni a munkavégzés megszervezésénél a „szükséges tudás" biztonsági alapelvet.
b) Ha nem tartózkodik senki a védett területen, akkor a területet biztonságosan le kell zárni, és rendszeresen ellenőrizni kell, hogy nem tartózkodik bent senki.
c) Harmadik fél alkalmazottja (kivéve az üzemlető alkalmazottját) szigorú szabályok szerint végezhet munkát a védett területeken:
    - Minden védett területen történő, harmadik fél bevonásával végzett munkavégzésről értesíteni kell az informatikust a munka megkezdése előtt 1 nappal.
    - Csak korlátozott ideig tartó felhatalmazás adható ki a munkavégzésre.
    - Felügyelet nélkül nem végezhet munkát harmadik fél alkalmazottja a védett területeken.
    - Ellenőrizni kell, hogy a munkát végző személynél csak a munkavégzéshez szükséges elektromos eszközök vannak. Tilos fotó, film, hangfelvétel, vagy egyéb adatrögzítésre, adattovábbításra alkalmas eszköz bevitele a védett területre.
d) Üzemidőn kívül az ajtókat zárva kell tartani.

e) A szerver szobában az esztétikus, higiénikus, folyamatos munkavégzés feltételeit kell megőrizni. A rend megtartásáért és a biztonságos műszaki üzemeltetésért a rendszergazdák a felelősek.
f) A szerver-szobába ételt, italt bevinni és ott elfogyasztani szigorúan TILOS!
g) Adathordozókat csak az informatikusok engedélyével lehet be- és kivinni a szerver szobából.

8.2. Berendezések védelme

8.2.1. Berendezések elhelyezése és védelme

Az eszközök elhelyezésénél figyelembe kell venni a biztonsági követelményeket, hogy a természeti hatásokból, a fizikai környezet változásaiból eredő kockázatok minimálisak legyenek. A megfelelő fizikai környezet megakadályozza a jogosulatlan hozzáférést is az informatikai eszközökhöz.

A Hivatal védelmének szempontjából az IV. és a V. biztonsági szinthez sorolt hálózati aktív eszközök esetében az alábbi rendelkezéseket kell betartani:

a) Az hálózati aktív eszközöket fizikai behatástól védett helyen kell tárolni.

b) Amelyik hálózati aktív eszköznél lehetséges, azt a switch szobában kell elhelyezni és a szerverekkel kapcsolatos biztonsági előírásokat kell betartani azokra vonatkozóan is.

A munkaállomásként üzemelő számítógépek fizikai hozzáférésénél az alábbi szabályokat kell betartani:

a) A munkaállomásokat zárható helyiségekben kell tárolni. Amikor egy helyiségben nem tartózkodik senki, az ajtót zárva kell tartani.

b) A tárgyaló helyiségekbe csak olyan munkaállomások kerülhetnek állandó elhelyezésre, amelyeken az operációs rendszeren és a kiszolgáló programokon kívül más alkalmazás nem kerül telepítésre, és csak a használatuk időtartama alatt lehetnek hálózatba kötve a felhasználó hozzáférési jogosultságának megfelelően. Ezen munkaállomásokra az egyes tárgyalások anyagai csak a tárgyalás időtartamára kerülhetnek fel.

A felhasználó informatikai eszközök nem mozgathatóak át más helyiségekbe, kivéve a hordozható számítógépeket. IT eszközök mozgatását csak az informatikus és a rendszergazdák végezhetik.

8.2.2. Kábelbiztonság

Az adatátvitelt bonyolító, illetőleg az információszolgáltatásokat támogató kábelhálózatot védeni kell a károsodástól.
Törekedni kell arra, hogy az elektromos hálózati kábeleket a falban legyenek vezetve, amennyiben ez nem megoldható, úgy vezetékcsatornában, a környezettől elzártan kell azokat vezetni. Törekedni kell arra, hogy az informatikai eszközök a lehető legrövidebb vezetékkel csatlakozzanak a falon vagy az álpadlóban kialakított csatlakozó aljzathoz.
Az adathálózati végpontokra idegen számítástechnikai eszköz csatlakoztatása külön engedély nélkül tilos. Erre vonatkozó engedélyt az informatikus adhat ki.

8.2.3. Berendezések karbantartása

A biztonsági követelmények (rendelkezésre állás, sértetlenség) teljesítése érdekében az eszközök rendszeres karbantartásáról gondoskodni kell.

c) A gyártó, beszállító által megadott időközönként, a megadott szempontok szerint kell karbantartani az eszközöket.

d) Csak arra felhatalmazott személy végezheti a karbantartást, és a szükséges javítási munkákat.

e) A hibákat, rendszerleállásokat, minden karbantartási tevékenységet dokumentálni kell.

f) Harmadik félnek javításra kiadott eszközökről, adathordozókról a minősített adatokat el kell távolítani, amennyiben lehetséges. Minősített adatokat tároló eszközök javításánál az információbiztonsági vezetőnek véleményezési joga van.

g) Amennyiben a Hivatal tulajdonában, bérletében lévő eszközt harmadik fél nem a Hivatal tulajdonában, bérletében lévő létesítményben karbantartja, javítja, gondoskodni kell az adattárolók biztonságos törléséről a kiszállítás előtt.

8.2.4. Berendezések biztonsága a telephelyen kívül

A cél, hogy a telephelyen kívüli berendezések kellő biztonságot nyújtsanak, figyelembe véve a Hivatal székhelyén kívül történő munkavégzésből eredő különböző kockázatokat. A Hivatal telephelyén kívül felhasznált informatikai eszközökre, adathordozókra is vonatkoznak a Hivatali információbiztonsági szabályok. Az informatikai eszközök, adathordozók lehetnek: személyi számítógépek, hordozható számítógépek, laptop-ok, mobiltelefonok, CD-k, DVD-k, mágnesszalagok, videoszalagok, papíralapú adathordozók, egyéb eszközök és adathordozók.

Épületből és Hivatal telephelyekről számítástechnikai eszközt kivitele

Felhatalmazás nélkül a Hivatal vagyonát képező eszközöket, információkat vagy szoftvereket tilos kivinni a telephelyről. Felhatalmazásnak minősül az aláírt átvételi elismervény laptop, és mobil eszközök esetén, beleértve az eszközön tárolt szoftvereket és adatokat is. Meghatározott, nagy értékű eszközök kivitelét és vissza hozatalát írásban rögzíteni kell. Szúrópróbaszerűen ellenőrizni kell a Hivatal vagyonának meglétét. Az érintett személyek tudomására kell hozni, hogy bármikor lehetséges ellenőrzés.

A számítástechnikai eszközök elvesztését, ellopását, megrongálódását haladéktalanul jelenteni kell az informatikai terület felügyeletével megbízott vezetőnek.

A hordozható számítógépek hazavitelére az alábbi rendelkezések érvényesek:

a) Az engedély alapján kiadott hordozható számítógépnek a leltárban is meg kell jelennie, és a felhasználó a számítógépet a leltározási időszakban köteles bemutatni.

b) Gondoskodni kell a hordozható számítógépek biztonságos szállításáról és tárolásáról. Biztosítani kell továbbá az illetéktelen hozzáférés megakadályozását, amelyért a felhasználó a személyében felelős.

c) Nyilvános helyen szigorúan tilos a Hivatallal kapcsolatos bizalmas adatokat, információkat tartalmazó hordozható számítógépet felügyelet nélkül hagyni.

8.2.5. Berendezések biztonságos selejtezése, illetve újrafelhasználása

Valamennyi olyan berendezést, amely tárolóeszközt foglal magában, ellenőrizni kell annak biztosítása érdekében, hogy az érzékeny adatok és engedélyezett szoftverek a selejtezést megelőzően eltávolításra, illetve biztonságos felülírásra kerüljenek. Az ellenőrzés végrehajtása a rendszergazdák feladata.

9. A kommunikáció és az üzemeltetés irányítása

9.1. Üzemeltetési eljárások és felelősségi körök

9.1.1. Dokumentált üzemeltetési eljárások

Gondoskodni kell az üzemeltetési eljárások dokumentálásáról és karbantartásáról, és minden olyan felhasználó számára hozzáférhetővé kell tenni, akinek arra szüksége van (pl.: rendszergazdák, alkalmazásgazdák). A dokumentumokat rendszeresen frissíteni kell és hivatalos, belső dokumentumként kell kezelni. Az üzemeltetési eljárások dokumentálását és karbantartását az informatikus végzi.

Az üzemeltetési eljárások az alábbi tevékenységeket öleli fel:

a) jogosultságok beállítása,

b) mentés, archiválás, visszatöltés, médiakezelés,

c) incidenskezelés,

d) rendkívüli helyzetkezelés és katasztrófa elhárítás tervezés.

e) hiba- és kivétel kezelési megoldások;

f) telefonszámok, elérhetőségek váratlan események esetére;

g) rendszer leállításának, újraindításának menete.

9.1.2. Változáskezelés

Az információ-feldolgozó eszközök és rendszerek változtatásaira vonatkozóan az alábbi alapvető előírásokat szükséges betartani:

a) Az éles rendszerhez történő illesztés előtt a változó komponenseket minden esetben tesztelés alá kell vetni.

b) A tesztelések eredményét dokumentálni kell.

Konfiguráció kezelés

Minden rendszer üzemeltetőjének szükséges az általa üzemeltetett szolgáltató rendszer és szolgáltatás esetében időrendben vezetni a konfigurációkezelési adatbázist. Amelynek tartalmaznia kell:
A változó komponens adatait
A változás indokát
A tesztelési adatokat
Az esetleges visszaállítási teendőket

Változás kezelés menete

Kritikus és kiemelt rendszer esetén a szolgáltatás üzemeltetője engedélyezteti a módosítani kívánt hardver és szoftver konfigurációt az illetékes szakértővel. Az engedélyezett változtatásokat a szolgáltatás üzemeltetője (az üzemeltetési leírásban leírt módon) végrehajtja, sikeres végrehajtás és teszt után a rendszer leírásában azt dokumentálja. A változtatásról az Biztonsági felelőst írásban tájékoztatni kell.

Sürgősségi változáskezelési eljárás

Azokat a változtatásokat, amik olyan hibák kijavítására irányulnak, melyek nagymértékben veszélyeztetik az informatikai szolgáltatást, és ezért a lehető legsürgősebben végre kell hajtani, sürgősségi változtatás keretében kell végrehajtani, amihez az illetékes szakértőn kívül biztonsági felelős engedélye is szükséges.

Hibajavítás

A Szervezet által használt kereskedelmi szoftvereinek hibáinak napvilágra kerülése esetén megnő a valószínűségen annak, hogy az támadók ezeket a biztonsági réseket/szoftver hibákat kihasználva próbálnak az információs rendszerébe behatolni, ezért elengedhetetlen, hogy a szoftver gyártója által készített javítások (frissítések) a lehető leghamarabb a telepítésre kerüljenek.

9.1.3. Az üzemeltetési feladatok, kötelezettségek elhatárolása

A feladatköröket és felelősségi területeket szét kell választani az informatikai erőforrásokhoz történő illetéktelen hozzáférés, illetve az azokkal való visszaélés megelőzése illetőleg e veszély minimalizálása érdekében. Az összeférhetetlen feladatok és felelősségek szétválasztását a Hivatal humán erőforrásainak figyelembe vételével kell alkalmazni. Korlátozott létszám esetén, amikor nem megoldható, hogy minden feladatot külön személy végezzen, megfelelő kereszt-ellenőrzéseket kell alkalmazni.

9.2. Harmadik felek szolgáltatásnyújtásának irányítása

9.2.1. Szolgáltatásnyújtás

A külső támogatást nyújtó szerződő partner általánosan a hardverrel és az operációs rendszerrel, az üzleti alkalmazásokkal, adatbázismotorokkal, valamint a hálózati kommunikáció lehetőségének biztosításával kapcsolatosan felmerülő kérdésekben jogosult a probléma megismerésére és megoldási javaslat benyújtására, kizárólag a szerződésben meghatározott szolgáltatás szerződésszerű teljesítése által indokolt mértékben.

A szerződésekben rögzített feltételek jogi megfelelőségéért (kikényszeríthetőségéért) a jogi referens, míg a szerződés informatikai szakmai tartalmáért, annak teljességéért, ideértve a szerződésszerű

szolgáltatás informatikai szakmai kritériumainak meghatározását, a szolgáltatás szakmai (minőségi) átvételének feltételeit is, az informatikus felel.

9.3. Rendszertervezés- és elfogadás

9.3.1. Rendszerek elfogadása, átvétele

Az informatikai rendszerek elfogadására és átvételére a dokumentált fejlesztői és felhasználói teszteket követően kerülhet sor. Az egyes rendszerek átvételének kritériumai rendszerenként egyedileg kerülnek meghatározásra.

9.4. Védelem a rosszindulatú és mobil kódok ellen

9.4.1. Rosszindulatú kód elleni intézkedések

A szerverek, kiszolgálók és munkaállomások vírusvédelmére különösen az alábbi rendelkezéseket kell betartani:

a) Minden munkaállomásra vírusellenőrző szoftvert kötelező telepíteni, melyért a rendszergazda felel.

b) A vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetében meg kell vizsgálnia az adathordozó tartalmát, és amennyiben vírust talált, nem engedhet másolást, futtatást a vírusok leirtásának megoldásáig.

c) A vírusellenőrző programnak központilag menedzselhetőnek kell lennie.

d) Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres – a gyártó által kibocsátott verziók telepítésével történő mielőbbi, legfeljebb 2 munkanapon belüli – frissítését.

e) A vírusvédő alkalmazást a levelező rendszerek központi szervereihez is integrálni kell.

f) A felhasználók részéről a vírusellenőrző szoftver beállításainak módosítása tilos.

g) Vírus felbukkanása esetén a szoftver kísérelje meg azt kiirtani, és értesítse a rendszergazdát, de legalább a felhasználót.

h) Kárt okozó, rendszerek működését befolyásoló esemény vagy vírusfertőzés esetén a felhasználó azonnal köteles értesítést küldeni a rendszergazda számára.

i) A vírusvédő alkalmazás vírusdefiníciós fájljainak naprakészségét, az automatikus frissítés helyes működését az üzemeltetést ellátó szolgáltató biztosítja, és a rendszergazda ellenőrzi.

9.4.2. Mobil kód elleni intézkedések

A Hivatal valamennyi munkaállomását vírusvédelmi rendszerrel kell ellátni. A rendszer telepítésének általános szabályai a következők:

a) A munkaállomáshoz csatlakoztatott tetszőleges adathordozó (például USB adathordozó), a csatlakozás pillanatában legyen teljes körűen ellenőrizve (on demand ellenőrzés);

b) A vírusvédelmi rendszernek minden állomány megnyitásakor el kell végeznie a vírusellenőrzést (on access ellenőrzés);

c) A vírusvédelmi rendszer épüljön be az elektronikus levelező és böngésző rendszerbe, minden állomány letöltés és feltöltés előtt végezze el a vírusellenőrzést, csatolt állományok esetében is;

d) A vírusvédelmi rendszert a felhasználó ne kapcsolhassa ki, beállításait ne változtathassa meg.

A vírusvédelmi rendszerrel kapcsolatos biztonsági standardokat jelen Szabályzat „D" melléklete tartalmazza.

9.5. Biztonsági mentés

9.5.1. Információk biztonsági mentése

A Hivatal számítógépein tárolt adatok védelmében meghatározó jelentőségű a biztonsági másolatok készítése. A mentés célja, egyrészt a ritkán használt adatok, illetve a kulcsfontosságú adatok (például adatbázis stb.) rendszerezett, biztonságos és visszakeresésre alkalmas tárolása, másrészt, hogy előre

nem látott adatsérülés, vagy adatvesztés esetén a sérült adatok a korábban szabályozott módon eltárolt mentésekből hiánytalanul visszaállíthatóak legyenek. Mentés során mind az egyes rendszerek adatait, mind az operációs rendszer, adatbázisrendszer és szoftverkörnyezet beállításait is tárolni kell.

A biztonsági mentésekre vonatkozó részletes előírásokat a *„Mentési terv"* című dokumentáció tartalmazza.

Rendszermérnök a dokumentációt havi ütemezéssel felülvizsgálja, azt naprakészen vezeti.

9.6. Hálózatbiztonság kezelése

9.6.1. Hálózatok védelme

A hálózatokat a fenyegetésektől való megóvásuk, és a hálózatot használó rendszerek és alkalmazások - ideértve az átvitel alatti információt – biztonságának fenntartása érdekében megfelelő irányítás és ellenőrzés alatt van tartva,port security segítségével.

9.6.2. Hálózati szolgáltatások biztonsága

A hálózat aktuális felépítéséről szerkezeti ábrát kell készíteni, melyben az alábbiaknak kell szerepelnie:

- Határvédelmi eszközök, és a hozzájuk kapcsolódó hálózati elemek
- Az összes aktív hálózati elem (switchek, routerek, média konverterek, átjárók);
- Szerverek, adattárak;

A fenti eszközök típusát, hálózati nevét, IP címét, valamint fizikai helyét is fel kell tüntetni. A III. biztonsági szintbe tartozó munkaállomásokat és egyéb informatikai eszközöket nem szükséges az ábrába beilleszteni, de folyamatosan regisztrálni kell, merre találhatók, és kik férhetnek hozzá.

A dokumentumot az informatikusnak kell karbantartania. A határvédelemmel kapcsolatos feladatok ellátásáért az informatikus felel, ellenőrzése az Informatikai biztonsági felelős feladata. Rendszermérnök a dokumentációt havi rendszerességgel frissíti.

9.6.3. Az eltávolítható adathordozók kezelése

A szállítás folyamán az adathordozót sérüléstől védő borítással kell ellátni. A beérkezett és kimenő adathordozón első és utolsó lépésben mindig vírusellenőrzést kell végezni.
Az adatok szállításának biztonságáról mindig az adattulajdonosnak kell gondoskodnia.

9.6.4. Adathordozók törlése

Amennyiben adathordozó eszközök újra felhasználásra kerülnek, úgy biztosítani kell, hogy az adathordozó új felhasználója jogosulatlanul ne férjen hozzá a korábbi adatokhoz. Ilyen esetben az eszközökön biztonságos törlést kell végrehajtani úgy, hogy a teljes adathordozón található valamennyi adat, kerüljön felülírásra véletlen adatfolyammal (pl.: Az ingyenes ccleaner program segítségével).
A törlést végző felelős a törlése sikerességért.
Amely adathordozókat, amelyeken nem lehet az engedélyezett törlést végrehajtani, újrafelhasználni, beépíteni tilos, ezeket le kell selejtezni, és meg kell semmisíteni.

9.6.5. Adathordozók selejtezése

A számítógépes feldolgozás során hibás, vagy feleslegessé vált, aktualitását vesztett mágneses és optikai adathordozókat selejtezés során kell megsemmisíteni. A selejtezés esetében az alábbi intézkedéseket kell betartani:

Amennyiben lehetőség van rá, a feleslegessé vált adathordozó (mágnesszalag, CD, DVD, optikai diszk, merevlemez/winchester) megsemmisítését a keletkezés helyén kell végrehajtani.
Amennyiben a feleslegessé vált adathordozó (mágneslemez, mágnesszalag, CD, DVD, optikai diszk, merevlemez/winchester) megsemmisítése a keletkezése helyén nem lehetséges, azok selejtezéséről az informatikus gondoskodik. A köztisztviselő köteles a munkája során keletkezett selejtezendő adathordozókat lezárt borítékban az informatikushoz eljuttatni.

Az adathordozókat úgy kell megsemmisíteni, hogy azok tartalmát illetéktelen semmilyen úton ne tudja újra olvasni, felhasználni.

10

A szoftver eszköz az alábbiak szerint semmisítendő meg:

- Az adathordozók és dokumentációk biztonságos daraboló, megsemmisítő berendezéssel.
- Mágneses adathordozókról (szalag, winchester, USB-s külső tárolók) a rajtuk tárolt adatok egy demagnetizálóval vagy a törléshez engedélyezett felülíró segédeszköz programmal.
- CD, DVD vagy egyéb optikai adattároló megsemmisítése az erre alkalmas daraboló eszköz alkalmazásával történhet.
- Adathordozók, és dokumentációk egy engedélyezett vállalkozó által végrehajtott elégetéssel.

A megsemmisítésről készült jegyzőkönyvnek tartalmaznia kell:

a) A megsemmisítendő adathordozók tulajdonosának megnevezését;

b) Milyen adathordozók és azon mely adatok kerültek selejtezésre;

A jegyzőkönyv 1 példányát az adathordozó tulajdonos szervezeti egysége, 1 példányát a megsemmisítést szervező informatikus ellenőrzi és irattárazza. A jegyzőkönyvek nem selejtezhetők.

9.6.6. Rendszerdokumentáció védelme

A rendszer dokumentációk tárolását korlátozott jogosultsággal elérhető mappában kell elektronikusan tárolni.
A rendszerdokumentációk tárolási rendszerének kialakítása, aktualizálása az üzemeltetést ellátó szolgáltató, ellenőrzése az informatikus feladata. A rendszerdokumentációk hálózati megosztott mappába történő feltöltéséért és a sértetlenség megőrzéséért az adatgazda felel. A dokumentációk rendelkezésre állásáért az Adatgazda és a Rendszergazda tartozik felelősséggel.

9.7. Információcsere

9.7.1. Fizikai adathordozók

A hordozható számítógépes eszközök (notebook, pendrive, DVD, CD) külső felhasználása során különös gondot kell fordítani az eszközök fizikai- és adatvédelmére.
A Hivatal tulajdonát képező adathordozók személyes célra történő használata tilos. A privát adathordozók munkahelyi használata külön engedélyhez kötött.
Az adatokról másolatok csak a munkafolyamatra vonatkozó előírásokkal összhangban készíthetők.

Az adatosztályozás szerint minősített adatokat csak nyilvántartott adathordozóra szabad felvinni. A nyilvántartott adathordozókat külön azonosítóval kell ellátni, ezeknek az azonosítóknak a feldolgozási, felhasználási folyamat végéig egyértelműen azonosíthatóknak kell lenniük és az adatvédelmi és adatbiztonsági előírások szerint kell őket kezelni.
Az adathordozók illetéktelen felhasználása elleni védelem az érintett munkatársak kötelessége és egyben felelőssége.

Ha a felhasználó azt észleli, hogy a hatályos belső vállalati szabályozó dokumentumokban foglaltak ellenére illetéktelen (jogosulatlan) adatmásolás történik, köteles erről a közvetlen felettesét késedelem nélkül értesíteni.

Az adathordozókat használaton kívül minden esetben el kell zárni.

A leselejtezett adathordozókat fizikailag meg kell semmisíteni.

Az adathordozók elvesztése esetén, amennyiben azokon nem publikus adatok voltak, haladéktalanul értesíteni kell az informatikust.

9.7.2. Az elektronikus levelezés biztonsága

Belső elektronikus levelezés szabályai

A Hivatal belső levelezésének elsődleges feladata a munkafolyamatok automatizálása, felgyorsítása.

Annak érdekében, hogy az elektronikus levelezés sértetlenségét és bizalmasságát a jelenlegi technológiai környezetben biztosítani lehessen, továbbá, hogy az e-mailezés valóban hatékony munkahelyi kommunikációs csatornává váljék, az alábbi szabályok betartására, betartatására kell figyelemmel lenni:

d) A munkatársak az egymás közötti elektronikus levélforgalmában kerülni kell a magántermészetű üzenetküldést,

e) A munkahelyi e-mail a munkáltató által a munkavégzéshez biztosított eszköz,

f) Az e-mail tárgy mezője legyen egyszerű és lényegre törő,

g) Az üzenetben kerüljük a nagy terjedelmű szöveg beillesztéseket, helyette mondanivalónkban utaljunk a levél csatolmányaként küldött dokumentumra

h) Amennyiben rögtön nem tudunk valamely email üzenetben kért feladattal foglalkozni, a feladót erről tájékoztassuk válaszlevélben,

i) Amennyiben a felhasználó több mint 24 óráig tervezi távolmaradását a számítógépétől, használja a "Házon kívül" automatikus választ.

j) A Hivatal által hivatalosan támogatott levelező rendszeren kívül más, elektronikus levelezést hivatalos kommunikációra, valamint a Hivatal munkaállomásait a munkakörhöz nem kapcsolódó feladatra használni tilos.

k) A felhasználók felelőssége a központilag tárolt postafiókokból kimentett és/vagy archivált levelek kezelése, hálózati (mentett!) mappába mentése.

l) Felhasználó tömeges levéltörlést nem végezhet.

Az informatikus jogosult az üzemeltetést ellátó szolgáltató javaslatai alapján meghatározni azoknak az információknak a körét, amelyek elektronikus levelezés útján történő forgalmazása korlátozható.

Elektronikus levelezés harmadik személlyel

A Hivataltól személyes adat, biztosítási titok, üzleti titok kizárólag akkor továbbítható – az egyéb feltételek fennállása mellett és előírások betartásával – harmadik személy számára elektronikus levélben, ha az elektronikus levelek minimum jelszavas védelme megoldott.

Amennyiben az adatszolgáltatás megkívánja és a befogadó fél fel van készülve a fogadására az elektronikus levelezésben digitális aláírást, illetve, ha szükséges időbélyegzést kel alkalmazni, vagy egész egyszerűen a fenti eszközökkel levédett ún e-dokumentumot (vagy XML fájl-t) kell elkészíteni és elküldeni a címzettnek.

Ahol nem szükséges a fenti szigorú védelmi és hitelesítési procedúra, vagy nem állnak készen a fenti módszerekkel védett levelek fogadására ott a csatolt mellékletek titkosítására van lehetőség „egységes" tömörítő program (WinZip), kellő titkosítási algoritmus (256bit, AES) és megfelelően bonyolult jelszó (legalább 10 karakter hosszú, kisbetű, nagybetű, szám karakterek) alkalmazásával. Természetesen a megadott jelszót - például SMS –ben, vagy normál levélben - a célszeméllyel közölni kell.

Az üzemeltetést ellátó szolgáltató az informatikus utasítására az egyes fájltípusok, illetve az ún.: „levélszemét" forgalmát a levelező szerver beállításaival letilthatja, vagy blokkolhatja. Amennyiben munkavégzési okból ilyen jellegű fájl forgalmára van szükség, a tiltás feloldását írásban kell kérni.

Az informatikus korlátozhatja a bejövő és küldhető fájlok méretét.

Mivel mind az e-mail, mind az internet forgalom a Hivatal által biztosított eszközökön történik, és ezen eszközök biztosítása a Hivatali folyamatok ellátásával kapcsolatos tevékenység megkönnyítésére irányul, az elektronikus levél – főszabály szerint – egy tekintet alá esik a Hivatalhoz érkező bármely más hivatalos irattal. A Hivatal első számú vezetőjének utasítására (polgármester és/vagy aljegyző) az informatikus elrendelheti az email címeken (azokról érkezett, vagy oda továbbított) bonyolított levelezés, továbbá az Interneten látogatott oldalak, temporális internet fájlok, letöltések ellenőrzését a felhasználó gépén, vagy a szerveren. Kivételt képeznek ez alól azok a levelek, amelyeket a felhasználó az ellenőrzés során magáncélúnak nyilvánít.

Elektronikus levelezés és az Internet oldalak látogatottságának ellenőrzése azonban csak akkor jogszerű, ha ezt a munkatársak előzetes tájékoztatása megelőzte.

Nyomós humán kockázati okból a magánjellegű levelezésbe a címzettjén kívül csak abban az esetben lehet betekinteni, ha alapos a gyanú, hogy a levél tartalma a Hivatal jogszerű pénzügyi, gazdasági vagy piaci érdekeit érinti.

A vállalati elektronikus levelezésről és az Internet használatának korlátairól, továbbá a munkatársakat megillető jogokról további rendelkezéseket tartalmaz az *„Iratkezelési szabályzat"* címmel kibocsátott – mindenkor hatályos – utasítás.

Az elektronikus levelezéssel kapcsolatos biztonsági standardokat jelen Szabályzat „C" melléklete tartalmazza.

9.7.3. Okostelefonok használata

A Hivatal az arra jogosult munkavállalóinak rendelkezésre bocsátott okostelefonok használatára vonatkozóan két biztonsági irányt határoz meg:

- védeni a telefont az illetéktelen hozzáféréstől
- védeni a vállalati hálózatot a kompromittált eszközöktől.

Az okostelefonok biztonságára vonatkozóan a Hivatal a következő előírásokat alkalmazza:

- Az okostelefonok menedzselését a Hivatal informatikusa vagy rendszergazdája végzi el,
- A készülékek egyedileg kerülnek azonosításra és felhasználókhoz rendelésre, amelyről nyilvántartás készül.
- A felhasználóknak az okostelefonokat jelszóval/jelkóddal kell védeniük.
- Az okostelefonokra vonatkozóan egységes alapbeállítások kerülnek alkalmazásra. A standard biztonsági beállításokat a felhasználók nem módosíthatják.

A készülék elhagyása, eltűnése, illetéktelen személy kezébe kerülése, illetve bármilyen meghibásodás észlelésének esetén azonnal értesíteni kell az üzemeltetést ellátó szolgáltatót az eseményről.

Az értesítést követően az üzemeltetést ellátó szolgáltató azonnal megkezdi a készülék és alkalmazásainak javítását, illetve letiltását.

A Hivatal az okostelefonok biztonságának növelése érdekében javasolja a következők betartását:

- A futó alkalmazások számának minimalizálása a nem használt alkalmazások kikapcsolásával,
- Bluetooth, Wi-Fi és GPS alkalmazások használatot követő kikapcsolása, mely jelentősen csökkenti az okostelefonok támadási felületeit.

9.8. Elektronikus kereskedelmi szolgáltatások

9.8.1. Nyilvánosan hozzáférhető információk

A nyilvánosan közzétett információk és a Hivatal weboldalán elhelyezett tartalom jelentős értéket képvisel az ügyfelekkel és a leendő ügyfelekkel való kapcsolattartás céljából. Ezért megfelelő biztonsági védelmet kell kidolgozni az ott megjelenített tartalmak hitelességének és rendelkezésre állásának biztosítása érdekében (hitelesített CA-tól szervertanúsítvány). A weboldal biztonságos üzemeltetésének ellenőrzése az Informatikai biztonsági felelős feladata.

9.9. Figyelemmel követés (monitoring)

9.9.1. Az informatikai rendszer naplózása

A számon kérhetőség és az auditálhatóság biztosítása érdekében olyan naplózási rendszert van kialakítva, mely lehetővé teszi a Hivatal informatikai rendszereiben bekövetkezett fontosabb események utólagos kivizsgálását, különös tekintettel az informatikai rendszerek biztonságát érintő eseményekre.

A Hivatal integrált naplógyűjtési és elemzési rendszert működtet.

A naplózást az alábbi 5 szinten kell megvalósítani:

- operációs rendszer

- Az operációs rendszerek maguk végzik a logolást, ezen logfájlok mentése az operációs rendszerrel együtt történik.

- adatbázis-kezelő
  - Az adatbázis kezelő beépített logolási rendszerrel rendelkezik, ezen logfájlok mentése az adatbázis mentéssel együtt történik.

- alkalmazói rendszer
  - Iktatórendszer belső logolást használ, mindent rögzít törölni nem lehet.
  - alapszabályként az alkalmazói rendszerek adatbázis szinten kerülnek logolásra
- határvédelmi eszközök
  - Naplógyűjtő eszköz: Wgdimension szerver
  - Naplózott

A naplóállományok gyűjtése hitelesített módon, időpecséttel ellátva van végrehajtva.

9.9.2. Órajelek szinkronizálása

A Hivatalon belül, illetőleg adott biztonsági tartományban működő valamennyi érintett információ-feldolgozó rendszer órajelét a Hivatal központi tartományvezérlőjéhez kell szinkronizálni. A rendszergazda felel azért, hogy ez a szinkronizáció megoldott legyen.

10. Hozzáférés-ellenőrzés

10.1. Felhasználói hozzáférés irányítása

10.1.1. Felhasználók regisztrálása, felhasználói jelszavak kezelése és ellenőrzése

A hozzáféréssel, azaz jogosultsággal kapcsolatos igényt, illetőleg módosítási igényt a Hivatal informatikusánál, a területi vezető aláírásával ellátott jogosultság igénylő lap leadásával kell kezdeményezni. Az üzemeltetést ellátó szolgáltató és az informatikus a közös fájl szerveren megtalálható Jogosultság Igénylő Lap(JIL)- jelen szabályzat „I" melléklete- alapján állítja be a jogosultság igényeket, és ellenőrzésük is erre vonatkozóan történhet.

10.2. Felhasználói felelősségek

10.2.1. Jelszóhasználat

Valamennyi felhasználó köteles a jelszavak kiválasztásában és használatában az elvárt biztonsági gyakorlatot követni. Minden felhasználó köteles védeni a jelszavát az illetéktelen hozzáféréstől. A felhasználók jelszavát a felhasználón kívül senki sem ismerheti, ideértve a rendszergazdákat is.

A jelszavak minimális hossza 8 karakter, és tartalmazniuk kell alfabetikus és numerikus karaktereket egyaránt. Tilos olyan jelszavakat alkalmazni, melyek könnyen kitalálhatóak, mint például a személyes adatok, egyértelmű dátumok vagy általános szavak (pl: "Budavár", password stb.). 8 elrontott jelszó próbálkozás után a felhasználói fiók 1 órára zárolásra kerül.

A jelszavakat 90 naponta automatikusan meg kell változtatni – erről a rendszer értesítést küld - , illetve akkor, ha a felhasználó úgy gondolja, hogy azok más tudomására juthattak.

Az utolsó 5 jelszót a rendszer eltárolja és új jelszó megadásakor ezektől különbözőt kell beállítani!

A munkaállomást mindig ki kell kapcsolni, és a hálózatról ki kell jelentkezni, ha a munka végeztével távozik a felhasználó.

Rendszerszintű jelszavak

Rendszer szintű jelszavaknak tekintjük azokat a jelszavakat, amelyek olyan azonosítóhoz tartoznak, amelyeket nem valamely felhasználó ismer és használ, hanem programok, például MS Windows 2012 R2 szolgáltatások (ú.n. service), ú.n. harmadik gyártótól származó programok (pl. Symantec Backup), speciális hardver elemek (menedzselhető SWITCH, hardveres tűzfal, stb.), illetve program modulok adatbázisokhoz való hozzáférése során használt jelszavak.

Amennyiben rendszergazdai teendők merülnek fel valamely felhasználó gépén, a felhasználó köteles együttműködni, és szükség esetén a rendszergazda rendszerbe történő belépését segíteni. Ha a felhasználó nem tartózkodik elérhető közelségben, a rendszergazda új, ideiglenes jelszót hoz létre a felhasználó számára, melynek segítségével elkészítheti a felhasználó személyes beállításait. Miután végzett a feladatával, a rendszert úgy kell beállítania, hogy a felhasználó az első bejelentkezésekor köteles legyen megváltoztatni a jelszavát.

A jelszót soron kívül meg kell változtatni, ha az illetéktelen (más) személy tudomására jutott, illetve juthatott, vagy a felhasználó azt elfelejtette.

A rendszer szintű jelszavak a rendszer installálása során a rendszergazda által kerülnek a rendszerbe. Ekkor a rendszergazda köteles az adott jelszót megváltoztatni és annak azonosítójával borítékban elhelyezni, a borítékot lezárni, és azon megjelölni a benne lévő azonosító funkcióját. A borítékokat a Hivatal felelős vezetője aláírással látja el, és kazettába zárva őrzi.

A rendszerszintű jelszavakat meg kell változtatni, ha a rendszergazda kilép, és már nem a Hivatal munkavállalója, szerződéses alkalmazottja!

10.2.2. Őrizetlenül hagyott felhasználói berendezések, tiszta képernyő politika

Amennyiben a felhasználó napközben magára hagyja a gépét, zárolást (Windows gomb + L) kell alkalmaznia. Az Active Directory-ban mindenki részére automatikus zárolást kell beállítani. A zárolást 30 perc időintervallum után kell aktivizálni.

10.3. Hálózati szintű hozzáférés ellenőrzés

10.3.1. Hálózati szolgáltatások használatára vonatkozó szabályzat

A határvédelem megfelelő üzemeltetése és működésének biztosítása érdekében a Hivatal mind a külső, mind pedig a belső hálózatának rendelkezésre állása és biztonságos működése is elengedhetetlen.

A felhasználók

A határvédelmi rendszer működtetésért az informatikus tartozik felelősséggel.
E körben köteles

a) a hálózat működőképességét folyamatosan felügyelni, a beérkező riasztásokat haladéktalanul kivizsgálni;

b) a Hivatal irodahelyiségeiben a LAN hálózat meghibásodása esetén a hibaelhárítást haladéktalanul megkezdeni;

c) az adathálózati aktív eszköz meghibásodása esetén haladéktalanul értesíteni a támogató céget, és utasítani a hibaelhárításra;

d) az előzőleg felsorolt eseményekről írásos feljegyzést készíteni, és a hibajavítás elvégzése után a munkalapot hitelesíteni és eljuttatni az Informatikai Biztonsági Felelőshöz(IBF);

10.3.2. Hálózathoz való csatlakozás ellenőrzése

Megosztott hálózatoknál, különösen azoknál, amelyek a szervezet határain túlra nyúlnak, a felhasználók jogosultságainak beállításával összhangban, korlátozni kell a hálózati csatlakozási képességét.

A korlátozásokat az informatikus menedzseli.

Hálózati forgalom analizálása, ellenőrzése érdekében a következők megtétele szükséges:

a) A rendelkezésre álló eszközök segítségével a Hivatal hálózatának, a vizsgálat ideje alatt történő hálózati forgalmának figyelése és az abban felbukkanó hibák, anomáliák vagy illegális tevékenységre utaló jelek keresése, valamint ezen túlmenően a hasonló jellegű anomáliák elhárítására tett intézkedések vizsgálata.

b) Inaktív hálózati felhasználók szűrése, ellenőrzése

c) A hálózatban nem használt, lejárt felhasználói nevek – accountok – és a felhasználói adminisztráció folyamatának vizsgálata.

d) Jogosulatlan hálózati bejelentkezések szűrése, ellenőrzése.

e) A jogosulatlan hálózati bejelentkezések, valamint jogosulatlan erőforrás-használati kísérletek feltárása és az elhárításukra tett intézkedések vizsgálata.

f) Hálózati megosztások ellenőrzése.

g) A számítógépes hálózatban üzemelő munkaállomásokon észlelt, adatállományok tárolására alkalmas megosztások – ún. share-ek – összevetése az engedélyezett megosztások listájával.

h) Nyitott portok szűrése, ellenőrzése.

i) A Hivatal szerverein, munkaállomásain található nyitott portok ellenőrzése és összevetése az engedélyezett portok listájával (router szabályok engedélyeivel). A felesleges, nem használt vagy informatikai- és adatbiztonsági veszélyeket jelentő nyitott portok megszüntetésének

kezdeményezése az illetékes informatikus, illetve felhasználói támogatást nyújtó munkatársak felé.

j) Tűzfal dokumentáció változás esetén történő aktualizálása.

k) Hálózati switch portok nyilvántartásának aktualizálása

10.3.3. Külső rendszerekből történő hozzáférés szabályozása

Külső cégek folyamatos üzemeltetési feladatainak ellátása érdekében (pl.: szerverek, alkalmazások karbantartása) a cégek megbízott munkatársai állandó távoli hozzáférést kaphatnak az általuk felügyelt rendszerhez. Ezeket a VPN hozzáféréseket a cégeknek az IBSz betartásával, bizalmasan és a szakmai normáknak megfelelően kell kezelniük.
Távoli hozzáférést kaphatnak a Szervezet azon munkatársai, akik a Szervezet által biztosított, távoli munkavégzésre alkalmas eszközzel rendelkeznek.
A kapcsolathoz használt jogosultságokat a szervezet informatikai szolgáltatás menedzsere adja ki.
A Szervezet informatikai infrastruktúráját távoli elérése csak titkosított kapcsolaton keresztül történhet. A rendszerhez történő csatlakozás csak a szükséges időre korlátozódhat, a munka végeztével a kapcsolatot bontani kell.

Az internet használatával kapcsolatos biztonsági standardokat jelen Szabályzat „B" melléklete tartalmazza.

11. Információs rendszerek beszerzése, fejlesztése és fenntartása

A Hivatal informatikusa évente feljegyzést készít az első számú vezető (jegyző) számára a külső szolgáltatók által biztosítandó informatikai szolgáltatások, a szállítókkal kialakítandó, vagy már meglévő technikai és szervezeti kapcsolat meghatározására. Az információs rendszerek beszerzésére, fejlesztésére és fenntartására vonatkozó külső szolgáltatókkal kialakított kapcsolatot írásbeli szerződésekben kell meghatározni, még a munkák megkezdése, illetőleg a beszerzések megtörténte előtt.

E szerződéseket oly módon kell előkészíteni, hogy az megfeleljen az általános üzleti normáknak, valamint jogi és belső szabályozási követelményeknek, beleértve különösen a biztonsági követelményeket (pl.: titoktartási nyilatkozat), illetve az anyagi, pénzügyi felelősségre vonatkozó követelményeket is. E szerződésnek nevesíteni kell azt a szerepkört betöltő munkavállalót is, aki felel a külső szolgáltató által nyújtott szolgáltatás teljesítésének folyamatos figyeléséről a szerződésben foglaltak betartásának ellenőrzése céljából.

A Hivatal az üzleti folyamatokat támogató alkalmazások fejlesztését külső fejlesztések útján valósítja meg.

A Hivatal működéséhez fejlesztett alkalmazások üzemeltetésére a következő szabályok vonatkoznak:

a) A fejlesztési-, a teszt-, és az éles környezetnek el kell különülnie.

b) A három környezetnek egymástól független gépeken / partíciókon (virtuális gépeken) kell futnia.

c) Minden alkalmazáshoz rendelni kell egy, az üzemeltetésért felelős rendszergazdát, továbbá az üzleti területről delegált adatgazdát.

d) A fejlesztők nem rendelkezhetnek jogosultsággal az éles alkalmazásokra.

Ha egy rendszert futtató szerver alap szoftvereiben, hardverkomponenseiben speciális javításokat, módosításokat kell végrehajtani, ezeket a rendszergazda csak az informatikus engedélyével végezheti el.
A javítások, módosítások, változtatások megtörténtét dokumentálni és - éles rendszer esetén – jegyzőkönyvezni is kell. Mindezért a rendszergazdák tartoznak felelősséggel. A verzióváltások rendjét a változáskezelési eljárások alapján kell elvégezni.

Amennyiben szükséges, a változásokról az érintett felhasználókat tájékoztatni kell, továbbá meg kell velük ismertetni a fejlesztés gyakorlati alkalmazásait és új lehetőségeit.

11.1. Információs rendszerek biztonsági követelményei

11.1.1. Biztonsági követelmények elemzése és meghatározása

Új rendszerek fejlesztésénél vagy a meglévő rendszerek bővítésénél a biztonsági követelményeket a megvalósíthatósági tanulmány részeként dokumentálni kell.

A biztonsági követelmények alapján meg kell határozni a szükséges kontrollokat, amit a felső vezetés jóváhagy. Az új üzleti alkalmazások szoftvercsomagjain biztonsági felmérést kell végezni, vagy független harmadik fél által minősített termékek használhatóak.

Az üzleti követelmények meghatározzák a kontrollokkal szemben támasztott követelményeket új rendszerek fejlesztésénél vagy a meglévő rendszerek bővítésénél. A biztonsági követelmények elemzése alapján határozhatóak meg a szükséges kontrollok.

11.2. Helyes információfeldolgozás az alkalmazásokban

11.2.1. Az adatfeldolgozás ellenőrzése

Az információ feldolgozási folyamat ellenőrzését a folyamatba épített kontrollok és a több szem elvén alapuló kontrollok megvalósításával kell biztosítani. A kontrollok megvalósítását a folyamat-ügyrendekben dokumentálni szükséges. Fontos, hogy a tranzakciót indító és engedélyező személye minden esetben elkülönüljön. Ezt a tevékenységet vezetői ellenőrzés keretében az érintett szakterület vezetője, illetőleg a belső kontroll funkció részeként a függetlenített belső ellenőrzés ellenőrizni köteles.

Az üzleti alkalmazásokba beépített ellenőrzési funkcióknak a bekerülő adatokat ellenőrizniük kell annak érdekében, hogy a feldolgozandó adatok között ne legyenek hibásak, vagy olyan a működést befolyásoló információk, amelyek az informatikai rendszer folyamatos és biztonságos üzemelését veszélyeztethetik. Az ellenőrzés kiemelkedően fontos az üzleti tranzakciók rögzítésénél, az állandó adatoknál (név és címadatok, pénzügyi limitek, beszállítók és vásárlók törzsszáma), a különböző paramétereket tartalmazó táblázatoknál (árlisták, árfolyamtáblázatok, adótáblázatok).

Ellenőrizni kell, hogy az adat

a) a megadott értékhatárok között legyen,

b) csak előre megadott karaktereket tartalmazhatnak az adat mezők,

c) nem hiányzik vagy hiányos.

11.2.2. A végfelhasználók által irodai alkalmazásokkal előállított dokumentumok kezelésének irányelvei

A Hivatal számára nagyon fontosak a felhasználók által előállított azon dokumentumok, melyeket nem a főfolyamatot támogató alkalmazói rendszereken keresztül állítanak elő, hanem a számítógépükre telepített sztenderd irodai alkalmazásokon (például MS Office) keresztül.

Ezeknek a dokumentumoknak a készítésére, tárolásukra és törlésükre az alábbi irányelvek alkalmazandók:

a) Minden üzleti információt tartalmazó dokumentációt a hálózati meghajtóra menteni.

- Saját dokumentumot „home" mappába-Z:meghajtó
- Szervezeti közös tároló – Y:meghajtó; ezen belül „Saját" megosztott mappa
- Többi szervezettel történő megosztás esetén: – Y:meghajtó; ezen belül „Kozos" megosztott mappa

b) A hálózati meghajtó ezen területéhez csak az arra felhatalmazottak férhetnek hozzá megfelelő jogosultság birtokában.

11.3. Rendszerfájlok biztonsága

11.3.1. Üzemelő szoftverek ellenőrzése

A jogtisztán beszerzett szoftverekről az informatikusnak naprakész nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a szoftver nevét, verzió számát, a szoftver vagy szoftver licenc darabszámát, a használat jogcímét (tulajdon, használati jog, bérleti jog), beszerzésének vagy térítésmentes használatba vételének időpontját, adott szoftver értékét, illetve az adott szoftver értékének kifizetésére utaló számviteli bizonylat azonosító adatát.

A nyilvántartást alá kell tudni támasztani az alkalmazott szoftver eszköz jogtisztaságát bizonyító szerződéssel vagy olyan szoftver fejlesztői nyilatkozattal, mely a térítésmentes felhasználást engedélyezi. A valóságban ténylegesen fellelhető és a nyilvántartásban szereplő szoftverek/szoftver licencek számának összehasonlítását az informatikus évente legalább egyszer köteles ellenőrizni, annak adatait Szoftverleltárban összesíteni.

A rendszergazdák által készített szoftverleltár felvételének megtörténtét, illetve annak megfelelőségét a Hivatal informatikusa ellenőrzi. Ha a szoftverleltár alapján jogosulatlanul használt szoftver kerülne feltárásra, akkor a informatikusnak vizsgálatot kell lefolytatnia a jogosulatlan szoftverfelhasználás tárgyában, és vizsgálnia kell azt is, hogy az adott szoftver használata elengedhetetlen-e, és ha igen, akkor gondoskodnia kell a szoftver használat jogszerűvé tételéről. Amennyiben a szoftver használata nem indokolt, akkor intézkednie kell a jogosulatlanul használt szoftver dokumentált törléséről. A vizsgálat elrendeléséről, eredményeiről az informatikusnak tájékoztatni kell az első számú vezetőt (jegyző) és a gazdasági igazgatót.

Az Informatikai biztonsági felelős feladata ellenőrizni az előírások betartását.

11.3.2. Programok forráskódjához való hozzáférés ellenőrzése

A Budapest Főváros I. kerület Budavári Polgármesteri Hivatalának keretein belül nem történik alkalmazásfejlesztés. Amennyiben erre mégis sor kerülne, akkor az egyedileg fejlesztetett szoftverek rendszerdokumentációinak és a programok forráskódjának verziókövetéssel együtt történő tárolását központi szerveren kell végrehajtani. A programok forráskönyvtárát kiemelt módon kell védeni. Csak felhatalmazott, megfelelő hozzáférési jogosultságokkal rendelkező személy olvashatja, módosíthatja a forrásfájlokat. Ahol lehetséges, a programok forráskönyvtára ne legyen része az éles környezetnek. A fejlesztés vagy karbantartás alatt lévő programok ne legyenek részei az éles környezet forráskönyvtárának. A programok forrásállományaihoz történő hozzáférést naplózni kell.

11.4. Biztonság a fejlesztési és támogató folyamatokban

11.4.1. Változás-szabályozási eljárások

Az informatikai rendszerek hibás működésének elkerüléséhez kiemelkedően fontos szigorú szabályok maradéktalan betartása a változások kezelésénél. Az informatikai rendszerek verzióváltása kidolgozott eljárások alapján megy végbe. Az informatikai rendszeren végzett minden változtatást dokumentálni kell. Az üzleti alkalmazás szoftverkomponenseinek változásai a működő környezet egyéb elemeinek biztonságos működésére is kihatással lehetnek, ezért amikor lehetséges és kivitelezhető, az alkalmazások és a működő környezet egyéb elemeinek változáskezelését egységesen kell kezelni.

a) A változást jóváhagyó engedélyeket tárolni kell, hogy szükség esetén elérhetőek legyenek.
b) Biztosítani kell, hogy a változást csak az arra felhatalmazott személy hajthatja végre.
c) Biztosítani kell, hogy a bevezetett változások nem érintik a rendszer sértetlenségét és biztonságát.
d) Minden komponenst – szoftvert, adatot, adatbázist, hardvert – azonosítani kell, amit érint a változás.
e) A munka elkezdése előtt az elvégzendő tevékenységeket dokumentálni kell. Ez alapján formális jóváhagyás szükséges.
f) Biztosítani kell, hogy a változtatás csak sikeres tesztelést követően történhessen meg. Amennyiben lehetséges a tesztelésbe az igénylést benyújtó, üzleti oldalt is be kell vonni. Ha erre nincs lehetőség, akkor a rendszer szállítójának kell az előzetes teszteket végrehajtania és dokumentálnia, valamint a verzió követési dokumentáció elkészítése. Az informatikus, illetve az informatikai biztonsági felelős a tesztelési jegyzőkönyvek és a verzió követési dokumentációk alapján dönt az adott rendszer élesbe állításáról.
g) Biztosítani kell, hogy a változás végrehajtása a lehető legkisebb leállással valósuljon meg.

h) Biztosítani kell, hogy az informatikai rendszer dokumentációja naprakész legyen. Minden változást dokumentálni kell.
i) Minden szoftver frissítés során az új rendszernek megfelelő verziószámot kell kapnia.
j) A változást generáló kéréseket fel kell jegyezni, és a feljegyzéseket meg kell őrizni.
k) Biztosítani kell, hogy az üzemeltetési dokumentáció és a felhasználói leírás naprakész legyen.
l) Biztosítani kell, hogy a változások végrehajtása ne zavarja az üzleti folyamatok működését.

Az operációs rendszer változása

Az informatika rendszerekben rendszeres időközönként szükséges az operációs rendszer frissítése, vagy új operációs rendszer telepítése. A fejlesztés, módosítás részeként az egyedi alkalmazásokat tesztelni, ellenőrizni kell, annak érdekében, hogy a változás ne veszélyeztetesse a helyes és biztonságos működést.

m) Az operációs rendszer változása nem befolyásolhatja az üzleti alkalmazás sértetlenségét és biztonságát szavatoló eljárásokat.
n) Az operációs rendszer változásának bejelentése után elég idő legyen a szükséges felülvizsgálatokra és tesztekre az implementálás előtt.
o) Biztosítani kell, hogy az üzletmenet folytonossági tervek is naprakészek maradjanak.

11.4.2. Alkalmazások műszaki átvizsgálása az üzemelő rendszerek megváltoztatását követően

Amikor üzemelő rendszerekben történik változtatás, a működés szempontjából kritikus alkalmazásokat át kell vizsgálni annak biztosítása érdekében, hogy a változtatás ne legyen hátrányos hatással a szervezet működésére, illetve a biztonságra.
A rendszertesztelésekkel kapcsolatos előírások a következők:

a) a teszt és az éles környezet elkülönítése,

b) a fejlesztő éles adatokhoz való hozzáférésének megakadályozása.

A rendszertesztelések kialakítása az informatikus, a felhasználói tesztek eljárásainak kialakítása az adatgazdák feladata. A tesztelések vezetői ellenőrzése az érintett szakterület vezetőinek, illetve a függetlenített informatikai ellenőrzés keretében az Informatikai biztonsági felelős feladata.

11.4.3. A rendszer fejlesztési életciklusa

Az informatikai eszközök különböző beszerzési eljárásmódjainak alkalmazásánál fokozottan szem előtt kell tartani, hogy a szóban forgó eszköz megfeleljen az IBSz szabályzatban rögzített informatikai biztonsági követelményeknek.
A Szervezet az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket. Fejlesztés esetén már a rendszer tervezésénél fokozottan figyelembe kell venni az informatikai biztonsági előírásokat, ajánlásokat. A Szervezet a fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket, valamint a szervezetre érvényes szabályok szerint kijelöli az ezen szerepköröket betöltő, felelős személyeket.
Az informatikai üzemeltetés az általa kiadott/telepített informatikai eszközökről (hardver, szoftver, fejlesztett rendszerek kiadása, telepítése, verziókövetés) naprakész nyilvántartást vezet *(\\bv-fs16\FS\INFORMATIKA\Sajat\TRACO\Riportok\hardver_leltar).*

11.5. Műszaki sebezhetőség kezelése

11.5.1. A műszaki sebezhetőségek vizsgálata

Az alkalmazásban lévő információs rendszerek műszaki sebezhetőségeiről aktuális információkat kell beszerezni és elemezni kell a Hivatal informatikai rendszerének az ilyen sebezhetőségekkel szembeni kiszolgáltatottságát. Az elemzések alapján megfelelő intézkedéseket kell hozni az ezzel járó kockázatok kezelésére.
A műszaki sebezhetőségek vizsgálatának végrehajtása az Informatikai biztonsági felelős feladata.

11.5.2. Belső és külső sebezhetőségi vizsgálatok lefolytatása

A sebezhetőségi vizsgálatok célja, hogy felderítse a Hivatal informatikai rendszerének külső és belső sebezhetőségeit, továbbá a hiányosságokból fakadó biztonsági kockázatok értékelése abból a szempontból, hogy az így felderített hiányosságok mekkora eséllyel lennének kihasználhatók a rendszerek elleni támadásra, adathozzáférésre, vagy más fenyegetettségre.

Ehhez egy feltételezett támadó által is használt módszereket és eszközöket kell alkalmazni, figyelembe véve természetesen, hogy a Hivatal infrastruktúrájában kár ne keletkezzen és az üzletmenetben se történjen fennakadás.

A külső és belső sebezhetőségi vizsgálatokat az informatikus utasítása szerinti időben kell elvégezni. A vizsgálatokat az informatikai infrastruktúrában, informatikai hálózatban bekövetkező jelentős változások esetén is végre kell hajtani. A vizsgálatokat dokumentált módszertan alapján kell végrehajtani. A tervezett módszertant a vizsgálatok megkezdése előtt az informatikus hagyja jóvá.

A módszertannak tartalmazni kell a következőket:

a) vizsgálatok architektúrája,
b) vizsgálatok feltételei,
c) végrehajtás lépései,
d) alkalmazott módszerek és eljárások,
e) vizsgálatok során felhasznált eszközök.
f) A vizsgálatok végrehajtásának módszertanában figyelembe kell venni az alábbi nemzetközi ajánlásokat:
g) OWASP (Open Web Application Security Project)
h) OSSTM (Open Source Security Testing Methodology)

A külső és belső sebezhetőségi vizsgálatok végrehajtása, jegyzőkönyv megírása, az Informatikai biztonsági felelős feladata.

11.6. Információbiztonsági incidensek kezelése

11.6.1. Információbiztonsági események és gyengeségek jelentése

A Hivatal minden alkalmazottjának és partnerének kötelessége az általa tapasztalt biztonsági eseményt vagy általa feltárt biztonsági sebezhetőséget haladéktalanul jelenteni az informatikusnak. Amennyiben a sebezhetőség (gyengeség) az informatikai szakterület munkatársainak magatartásában (tevékenységében vagy mulasztásában) tapasztalható, a jelentést az első számú vezető, távolléte esetén az Informatikai biztonsági felelős részére kell megtenni.

A szoftverek használata során tapasztalható rendellenességeket azonnal jelenteni kell a munkahelyi vezetőnek, illetve az informatikusnak. A jelentésnek tartalmaznia kell a rendellenes működés leírását, az üzeneteket, kimeneti adatokat fel kell jegyezni.

A biztonsági események kezelése, azok elhárítása során szerzett tapasztalatokat rendszerezni kell, hogy azok felhasználhatóak legyenek egy újabb esemény hatékonyabb elhárítása során. A tapasztalatokat bizalmasan kell kezelni, mivel a bennük szereplő információk a Hivatal sérülékeny pontjairól tartalmaznak adatokat.

12. Működés folytonosságának irányítása

12.1. A működés folytonossága irányításának információbiztonsági szempontjai

A Hivatal nagy hangsúlyt fektet az informatikai rendszereinek esetleges kiesése esetén azok mielőbbi visszaállítására. Ezt Katasztrófa Elhárítás Tervezési (DRP) Szabályzatában írja elő. Az hivatali tevékenység folyamatosságának a fenntartására irányuló előírások célja annak biztosítása, hogy valamilyen elemi katasztrófa vagy a számítástechnikai rendszerek működésében beállt zavar okozta leállás után az alapvető üzleti műveletek sikeresen fenntarthatóak illetve újraindíthatóak legyenek.

12.2. Az információbiztonság a működésfolytonosság irányítás folyamatában

A Hivatal működésfolytonosságának biztosítása érdekében kiemelt szerepet kap az informatikai biztonság és a kockázatokkal arányos védelem.
A működés folytonosság tervezésének célja a működés fennakadásainak kivédése, a kritikus működési folyamatok megvédése az információs rendszerek nagyobb meghibásodásainak hatásaitól, illetve a rendszerkatasztrófáktól, valamint azok megfelelő időben történő újraindításának biztosítása. Ennek érdekében meg kell határozni a kritikus fontosságú üzleti funkciókat, alkalmazásokat és támogató technológiákat, valamint:

a) Költség hatékony újraindulási stratégiát kell kifejleszteni.
b) Alternatív tartalékként működő telephelyet kell meghatározni, amely rendelkezik a szükséges megfelelő infrastruktúrával, és támogatni tudja a rendszer újraindítási igényeket.
c) Meg kell határozni a katasztrófa elhárító és a rendszert újraindító munkacsapatok tagjait és vezetését.
d) A rendszer (katasztrófa helyzetet vagy valamilyen rendszer meghibásodás elhárítását követő) újraindításához szükséges intézkedések meghatározása és a rendszer újraindításához szükséges valamennyi erőforrás meghatározása, valamint azok biztosítása, továbbá az említett információknak a rendszer újraindítási terv keretében történő összeszerkesztése.
e) A (katasztrófa elhárítást végző és a) rendszert újraindító munkacsapatok megfelelő felkészítése a rájuk váró feladatok elvégzésére.
f) Meg kell határozni a rendszer szállítójának a rendszer újraindításban történő részvételi képességét.
g) Folyamatos ellenőrző és karbantartási programot kell kifejleszteni, amely biztosítani tudja, hogy a Hivatal informatikai rendszerei bármikor újraindításra képes állapotban legyenek.

12.3. Az információbiztonságot magukban foglaló folytonossági tervek kidolgozása, megvalósítása, tesztelése

Szakterületenként a kritikus folyamatokat érintő rendkívüli helyzetek esetére részletes cselekvési tervet kell készíteni, amelyben a rendkívüli helyzetek kezelésére vonatkozóan konkrét feladatokat, utasításokat kell megfogalmazni. A kritikus folyamatokat támogató informatikai rendszerek, rendkívüli helyzeteket követő visszaállításáról gondoskodni kell. A visszaállítási tervek tesztelését rendszeresen (évente egy alkalommal) el kell végezni.

12.4. Üzletmenet folytonossági tervek vizsgálata, fenntartása és újraértékelése

Az üzletmenet folytonossági tervek kidolgozását (felelős az aljegyző és az irodavezetők) követően folyamatosan gondoskodni kell azok aktualizálásáról, a változó környezeti feltételek, technikai fejlesztések és egyéb erőforrás-változások figyelembevételével.
A rendkívüli esemény bekövetkezésekor alkalmazandó eljárások, valamint az ezek megvalósításához szükséges erőforrás és egyéb feltételek, adatok aktualizálását éves rendszeres felülvizsgálat keretében kell elvégezni.

Minden, a Hivatal BCP és DRP tervezésével és szabályozásával kapcsolatos aktuális dokumentumot elérhetővé kell tenni a belső hálózat arra kijelölt mappájában.

12.5. Rendszer karbantartási eljárásrend

A Szervezet:

- megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint a szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer karbantartási eljárásrendet.

- **Rendszeres karbantartás**

A Szervezet:

- a karbantartásokat és javításokat ütemezetten hajtja végre

Rendszer	Karbantartás	Gyakoriság	Időtartam	Dátum	Felelős
Szerverek	**tisztítás, restart**	**Éves**	**1óra**	**2018.03**	**Rendszergazda**
Munkaállomások	tisztítás, restart	Éves	1óra	2018.03	Rendszergzada
Hálózati eszközök	**tisztítás, restart**	**Éves**	**1/2óra**	**2018.03**	**Rendszergazda**
Nyomatók	tisztítás, restart	Éves	½ óra	2018.03	Rendszergazda

- dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a szervezeti követelményeknek megfelelően.
- jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban
- az elszállítás előtt minden adatot és információt – mentést követően – töröl a berendezésről;
- ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
- csatolja a kitöltött karbantartási naplót (IBSz J melléklet) a karbantartási nyilvántartáshoz

13. Jogszabályoknak és szabványoknak való megfelelés, és műszaki megfelelőség

Az IBSz-be foglalt szabályoknak és a Hivatal működésének meg kell felelnie a vonatkozó törvényi előírásoknak és jogszabályoknak. Az IBSz figyelemmel van a vonatkozó szabványokra és ajánlásokra is.

13.1. Jogszabályok

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;
- 2012. évi C. törvény a Büntető Törvénykönyvről;
- 218/1999. (XII. 28.) Korm. rendelet az egyes szabálysértésekről;
- 79/1995. (VI. 30.) Korm. rendelet a minősített adatok kezelésének rendjéről.
- 2012. évi I. törvény a Munka törvénykönyvéről (a továbbiakban: Mt.)
- 1992. évi LXIII. törvény a személyi adatok védelméről és a közérdekű adatok nyilvánosságáról szóló
- 84/2007. (IV. 25.) Korm. rendelet a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről
- 2004. évi CXL. törvény (Ket.) a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól
- 335/2005. (XII. 29.) Korm. rendelet 66. §. a közfeladatot ellátó szervek iratkezelésének általános követelményeiről
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

13.2. Szabványok

- MSZ EN ISO 17799;
- MSZ ISO/IEC 27001:2006.
- RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- Miniszterelnöki Hivatal Informatikai Koordinációs Iroda - Informatikai biztonsági módszertani kézikönyv 8.sz. ajánlás
- ISACA ajánlásai (COBIT)

13.3. Az IBSz-hez kapcsolódó belső szabályozók és alkalmazott módszertanok jegyzéke

Dokumentum neve	Dokumentum típusa, jellege
Szervezeti és Működési szabályzat	Utasítás
Archiválási Szabályzat	Utasítás
Iratkezelési szabályzat	Utasítás
Tűzvédelmi szabályzat	Utasítás
Katasztrófa elhárítási terv	dokumentáció
Adatmentési terv	dokumentáció
Képzési eljárási rend	dokumentáció
Konfigurációkezelés	dokumentáció
Rendszerbiztonsági terv	dokumentáció
Rendszerfelügyelet	dokumentáció

"A" melléklet - A szabályzatban használt fogalmak meghatározásai

E szabályzat alkalmazása során előforduló legfontosabb informatikai, informatikai biztonsági, adatvédelmi és adatbiztonsági fogalmak:

adat: Az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája;

adatállomány: Valamely informatikai rendszerben lévő adatok logikai vagy fizikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz;

adatgazda: az a személy, aki élve a pénzügyi intézmény által biztosított jogosultságával adatot minősít, illetve osztályba sorol és felelős az általa minősített adat kezeléséért;

adatbázis: Elektronikus formában, digitálisan tárolt információk összessége

adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől;

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet aki, vagy amely az adatkezelő megbízásából - beleértve a jogszabály rendelkezése alapján történő megbízást is - személyes adatok feldolgozását végzi;

adatkezelés: az alkalmazott eljárástól függetlenül a személyes adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is;
A Hivatalnál személyes adatkezelést végeznek a munkaügyi és az üzleti nyilvántartásokat vezető munkatársak is.

adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet aki, vagy amely a személyes adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;

adatmegsemmisítés: az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése;

adattovábbítás: ha az adatot meghatározott harmadik személy, vagy alkalmazás számára hozzáférhetővé teszik;

adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

adatvédelem: Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire vonatkozik

adatzárolás: az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele;

alapfenyegetettségek: A fenyegetések általánosított csoportosítása. Ide soroljuk: a bizalmasság, a hitelesség, a sértetlenség, a letagadhatatlanság, a rendelkezésre állás és a funkcionalitás sérülését vagy elvesztését;

alkalmazás: alkalmazáson a pénzügyi intézmény valamely üzleti célja megvalósítása vagy megvalósulásának támogatása érdekében elkülönülő, saját néven egységbe szervezett hardver-szoftver-kommunikációs erőforrásainak együttesét értjük. Az alkalmazásokra az ember-számítógép együttműködés jellemző. Az alkalmazáshoz tartozónak tekintjük a tevékenységet támogató/hordozó, meghatározott üzleti-, banki-, szervezeti-, stb. cél elérése érdekében a pénzügyi szervezet teljes informatikai rendszerére alapozva kidolgozott technológiát ("know-how"-t) valamint a beépített elméleti modellt az alkalmazás dokumentációjával együtt;

átlagos helyreállítási idő: A hibák behatárolására és megszüntetésére fordított kényszerű leállások átlagos ideje;

archiválás: Az alkalmazás (tágabb értelemben az informatikai rendszer) egy-egy környezetének (tehát nem csak adattartalmának) különleges mentése. Különleges, mivel az archivált és a visszamaradó rendszernek is logikailag épnek, visszaállíthatónak kell lennie. Az archiválás — ellentétben a mentéssel — általában nem elsősorban biztonsági, hanem hatékonyság javító üzemviteli intézkedés (legtöbbször a visszamaradó környezet/rendszer felgyorsítása érdekében);

backup rendszer: Az informatikai biztonság megvalósítása során az adatok rendelkezésre állását lehetővé tevő másolatokat őrző rendszer. Rendszerint minimális tartalékkal rendelkező informatikai rendszert is értenek alatta;

banktitok: minden olyan, az egyes ügyfelekről a Hivatal rendelkezésére álló tény, információ, megoldás vagy adat, amely az ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint pénzügyi számlájának egyenlegére, forgalmára, továbbá a Hivatallal kötött szerződéseire vonatkozik;

bizalmasság: (szervezeti állapot) A pénzügyi intézmény olyan állapota, amely biztosítja, hogy az adatokhoz csak azok a meghatalmazottak férhessenek hozzá, akiknek a szervezet ehhez jogot adott. (adat tulajdonság) A ~bizalmasság a kezelőrendszer által az adatokhoz rendelt tulajdonság, amely jelzi/kifejezi az adat osztályba sorolásának megfelelő védelmi intézkedések teljesülését. Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról;

biztonság: olyan szervezeti állapot, melyben az adott szervezetnek a lehető legkisebb veszélyekkel kell számolnia, szolgáltatásait a vállalt/előírt feltételekkel és korlátozások nélkül képes nyújtani, a feladatait, funkcióinak ellátását illetően érdemi hatást gyakorló veszteség nem éri, a lehetséges fenyegetettségek bekövetkezési valószínűségéből és a lehetséges kárértékekből származtatott kockázat a szervezet számára elfogadhatóan alacsony, és a kockázatkezelési eljárások eredményeként kialakuló maradvány kockázat a szervezet számára az elviselhető tartományban marad. A védeni kívánt informatikai rendszer olyan, az adott intézmény számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg. A biztonság az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik;

biztonsági auditálás: Az informatikai rendszerre vonatkozó feljegyzések és tevékenységek független átvizsgálása, a rend-szer ellenőrzések megfelelőségének vizsgálata, a kialakított szabályzatok és a működtetési eljárások megfelelőségének elérése, a biztonság gyenge pontjainak felfedése az ellenőrzésben, a szabályzatokban és az eljárásokban ajánlott biztonsági változtatások céljából;

biztonsági esemény: Az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, amelynek hatására az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült vagy megsérülhet;

biztonsági kockázat (informatikai kockázat): valószínűségi mérték, amely az informatikai rend-szer működését veszélyeztető valamely körülmény bekövetkezési valószínűségével , illetve a be-következéskor várható kár nagyságával egyaránt arányos. Rendre élőmunka igényben, időben, pénzben vagy ezek együttesében fejezhető ki;

biztonsági követelmények: A kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági szükségletek együttese;

biztonsági rés: Az informatikai rendszer védelme érdekében a legkülönbözőbb területeken kell intézkedéseket hozni. A megelőző, elővigyázatossági intézkedések érinthetik az építészeti, a műszaki, a szervezési és a személyi kérdéseket. Az intézkedéseket egymással össze kell hangolni, és egy informatikai bizton-sági szabályozási rendszerben kell összefoglalni. Tudatában kell lenni annak, hogy – mint általában – egyetlen informatikai rendszer biztonsága sem lehet száz százalékos. Tökéletes megoldás nem létezik. Az értelemszerűen fennmaradó maradványkockázatokat azonban ismerni kell, és figyelem-be kell venni. A szabályozási rendszer kidolgozásakor a cél ezen maradványkockázatok elviselhető szintre szorítása. A védelmi igény mértéke függ a bevezetendő informatikai rendszer tulajdonságaitól és a bevezetés környezetétől is;

CA : Certification Authority (lásd *Hitelesítés Szolgáltató*);

Cracker: Az informatikai rendszerbe informatikai eszközöket használva, direkt rombolási céllal betörő személy;

CRAMM: CCTA Risk Analysis and Management Method. Az Egyesült Királyság Central Computer and Telecommunication Agency szervezete által kidolgozott kockázatelemzési és kezelési módszertan;

DEMO szoftver: Számos licence köteles szoftver gyártója ingyenesen vagy csekély költség ellenében (demonstrációs azaz demo) próbaverziókat bocsát ki. E szoftverek célja a bemutatás, tesztelés és kipróbálás, ennek megfelelően funkcionalitásuk sok esetben nem teljes, és használatuk általában időkorláthoz kötött. Ezeket a szoftververziókat tilos üzleti célra felhasználni;

Digitális aláírás: (Lásd *Elektronikus aláírás.)*

egyszeri javítási idő: Az informatikai rendszer egyszeri javítási ideje, amely a hiba észlelésétől az informatikai rendszer normál üzembe való visszatéréséig tart;

elektronikus aláírás: Az informatikai rendszerben kezelt adathoz rendelt, kódolással előállított olyan jelsorozat, amely az adat hitelességének és sértetlenségének bizonyítására használható;

elérhetőség: Az az állapot, amikor az információ feldolgozás során valamely informatikai alkalmazás szolgáltatásai az adott helyen és az adott időben igénybe vehetők.

ellenőrzési nyom: Az informatikai tevékenységek rögzítésére szolgál, amelynek alapján az illegális, illetve nem meg-felelő tevékenységek feltárásra, jelentésre kerülhetnek.

érték: Az információk és feldolgozásuk értéke abból vezethető le, hogy azok milyen jelentőséggel rendelkeznek a felhasználó által támasztott követelmények kielégítése szempontjából. Az informatikai rendszerelemek értéke pedig azon információk és feldolgozásuk értékéből származtatható, amelyek az adott rendszerelem igénybevételével megvalósuló eljárásokban részt vesznek;

feladatelhatárolás: Az informatikai rendszer használatához és üzemeltetéséhez kapcsolódó biztonságkritikus munkakörök szétválasztása;

felelősségre vonhatóság: Olyan tulajdonság, amely lehetővé teszi, hogy egy adott folyamat tevékenységei egyértelműen az adott folyamatra legyenek visszavezethetők.

felhasználó: Az a személy, szervezet vagy csoport, aki (amely) egy vagy több informatikai rendszert igénybe vesz feladatai megoldásához.

felhasználói hitelesítés: A felhasználó hitelességének ellenőrzése (a belépéskor minden felhasználó ellenőrzése), és különböző azonosító eszközök (pl.: jelszó, chip-kártya, biometrikus azonosítás stb.) alkalmazása;

fenyegetés: A biztonság megsértésének lehetősége;

fenyegetettség: Olyan állapot, amelyben az erőforrások felfedésre, módosításra vagy elpusztításra kerülhetnek;

fenyegető tényező: Olyan körülmény vagy esemény, amely az adat, illetve információ valamely informatikai rendszerben történő feldolgozásának rendelkezésre állását, sértetlenségét, bizalmasságát vagy hitelességét, illetve az informatikai rendszernek és a rendszer elemeinek működőképességét fenyegetheti. A fenyegető tényezők közé soroljuk nemcsak a személyektől eredő támadásokat, amelyek valamely informatikai rendszer ellen irányulnak, hanem valamennyi szélesebb értelemben vett fenyegetést, mint például véletlen eseményeket, külső tényezők általi behatásokat és olyan körülményeket, amelyek általában magának az informatikának a sajátosságaiból adódnak. (Példaként említhetjük a tüzet, az áramkimaradást, az adatbeviteli hibát, a hibás kezelést, a hardver tönkremenetelét, a számítógépes vírusokat és a különböző programhibákat.);

féreg program: Olyan programtörzs, amely az informatikai hálózaton keresztül terjed, jut el egyik informatikai rendszerből a másikba, és fejt ki kártékony hatását;

fizikai biztonság: Erőforrások szándékos és véletlen fenyegetései elleni fizikai védelemre használt intézkedések, illet-ve az anyagi térben megvalósuló szándékos vagy véletlen támadások elleni védelem.

folyamatosság: Az üzleti tevékenységek zavarmentes rendelkezésre állása;

folytonos védelem: Olyan védelmi megoldás, amely az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul;

Freeware szoftver: Olyan ingyenesen, licence kötelezettség nélkül használható szoftver, amelynek alkotói lemondtak a szerzői jogi védelemről;

funkcionalitás: Az informatikai rendszerelem (beleértve az adatokat is) olyan tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a kezelési céloknak megfelel, és használható;

gyenge pont: Az informatikai rendszerelemek olyan részei vagy tulajdonságai, amelyek révén a fenyegető tényezők hatásainak ki vannak téve;

Hacker: Az informatikai rendszerbe informatikai eszközöket használva, kifejezetten ártó szándék nélküli betörő személy;

hálózat: Számítógépek (vagy általánosabban informatikai rendszerek) összekapcsolása, és az összekapcsolt rendszerek legkülönbözőbb komponensei közötti adatcserét megvalósító logikai és fizikai eszközök összessége;

Hitelesítés Szolgáltató: (CA – Certification Authority) Olyan mindenki által megbízhatónak tartott, szakosodott szervezet, amely tanúsítványokat adhat ki kliensek és szerverek számára.

hitelesség: Egy adat hiteles, ha minden kétséget kizáróan megállapítható annak előállítója és az a tény, hogy az az előállítás óta változatlan maradt. A hitelesség tehát az adat (és az adathordozó) tulajdonsága, amellyel igazolhatjuk, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

hozzáférés: Olyan eljárás, amely valamely informatikai rendszer használója számára – jogosultságának függvényében - meghatározott célra, helyen és időben elérhetővé teszi az informatikai rendszer erőforrásait, elérhetővé tesz a rendszerben adatokként tárolt információkat. Ez az eljárás bekövetkezhet például névmegadáson keresztül valamely adatszerűségre nézve, és lehetővé tehet olvasást, írást vagy akár törlést is.

hozzáférés ellenőrzés: Az informatikai erőforrásokhoz való jogosulatlan hozzáférések elhárítása, beleértve az erőforrások jogosulatlan használatának megakadályozását is.

hozzáférés ellenőrzési lista: Az informatikai erőforrásokhoz való hozzáférésre jogosult entitások és hozzáférési jogaik jegyzéke.

humánbiztonság: Az erőforrások bizalmasságának és/vagy sértetlenségének és/vagy rendelkezésre állásának sérelmére – az intézménnyel munkaviszonyban álló vagy az intézménynél bármely szerződés alapján tevékenységet folytató vagy külső személyek által – elkövethető szándékos vagy véletlen humántámadások elleni védettség;

illegális szoftver: Az a szerzői jog védelme alatt álló szoftvertermék, amelynek a legalitás igazolásához szükséges dokumentumok (licence, számla, szállítólevél, ajándékozási szerződés stb.) nem mindegyike áll rendelkezésre, valamint a szoftver használata nem felel meg a licence szerződés előírásainak.

illetéktelen személy: Olyan személy, aki az adat megismerésére nem jogosult.

informatika: A számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.

informatikai biztonság: A pénzügyi intézmény informatikai rendszerének olyan kielégítő állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és

rendelkezésre állása, illetve az informatikai rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

informatika-biztonsági felelős: Olyan személy, aki a pénzügyi intézményen belüli biztonság megvalósításáért felel. Részt vesz az informatika biztonsági politika és szabályozás kidolgozásában, oktatásában, aktualizálásában, felelős annak ellenőrzésében és betartatásában.

informatika-biztonsági terv: Olyan az éves informatikai terv részét képező költségvetési és egyéb erőforrásokra vonatkozó, az IT biztonsággal kapcsolatos hardver-, szoftver-, oktatási-, szabályozási- és egyéb dokumentumok.

informatikai rendszer: A hardver-, szoftver- kommunikációs eszközök és ezek kezelő/kiszolgáló szervezeteinek olyan együttese, amelyet a pénzügyi intézmény üzletpolitikájával összhangban céljai megvalósítására használ.

informatikai katasztrófa: Egy olyan nem kívánt esemény, amely az adattovábbító, -tároló és -feldolgozó képesség elvesztését okozza hosszabb időre.

informatikai katasztrófahelyzet: Az az állapot, amikor egy rendszer utolsó működőképes állapotát a megállapított helyreállítási időn belül nem lehet visszaállítani.

informatikai katasztrófa utáni helyreállítási terv: Eljárás vagy tevékenység lépések sorozata annak biztosítására, hogy a szervezet kritikus információ feldolgozó képességeit katasztrófa után, a szükséges aktuális adatokkal helyre lehessen állítani elfogadhatóan rövid idő alatt.

informatikai rendszer: Információs, ügyviteli, üzletviteli vagy folyamatot, szolgáltatás működését támogató elektronikus adatfeldolgozó eszközök és eljárások, valamint az ezeket kiszolgáló emberi erőforrások és a kapcsolódó folyamatok összessége.

informatikai vészhelyzet: Egy olyan nem kívánt állapot, amely az intézmény rendelkezésére álló informatikai biztonsági rendszer szabályainak előírásszerű betartásával és végrehajtásával, a meghatározott erőforrások felhasználásával meghatározott időn belül megoldható.

információ: Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott olyan megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg. Az információ általános értelemben a valóság folyamatairól és dologi viszonyairól szóló felvilágosítás.

információrendszer: Információk meghatározott célú, módszeres gyűjtésére, tárolására, feldolgozására (bevitelére, módosítására, rendszerezésére, aggregálására) továbbítására, fogadására, megjelenítésére, megsemmisítésére stb. alkalmas rendszer. Ha ez a rendszer számítógéppel támogatott, akkor számítógépes információrendszerről (informatikai rendszerről) beszélünk.

információvédelem: Az informatikai rendszerek által kezelt adatok által hordozott információk bizalmasságának, hite-lességének és sértetlenségének védelme.

irányelvek: A szervezet vezetése által is elfogadott, követett és kommunikált általános szabályok ismertetése. A szabályozási struktúra legfelsőbb szintje, amelynek részletes megvalósítása a szabályozási struktúra további elemeiben (utasítások, körlevelek, szabályzatok, eljárásrendek, kézikönyvek, stb.) találhatók meg.

irat: minden olyan szöveg, számadatsor, térkép, tervrajz és vázlat – a megjelentetés szándékával készült könyv jellegű kézirat kivételével –, amely valamely szerv működésével, illetőleg személy tevékenységével kapcsolatban bármilyen anyagon, alakban, bármely eszköz felhasználásával és bármely eljárással keletkezett;

jogosultság: A lehetőség megadása az informatikai rendszerben végzendő tevékenységek végrehajtására;

jogosultsággal rendelkező felhasználó: Egy olyan felhasználó, aki jogosult egy tevékenység végrehajtására;

katasztrófa: Az informatikai rendszer folyamatos és rendeltetésszerű működésének megszakadása.

kár: Azon érték csökkenése, amelyet valamely objektum jelent egy informatikai rendszer alkalmazásában és amely akkor következik be, ha valamely fenyegető tényező kifejti hatását.

kockázat: Az informatikai fenyegetettség mértéke, amely valamely fenyegető tényezőből ered és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat két részből, a kárnagyságból és a bekövetkezés gyakoriságából tevődik össze.

kockázatelemzés: Olyan elemző és értékelő jellegű szakértői vizsgálat, amely az informatikai rendszerekben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a potenciális kárértékeket és azok bekövetkezési gyakoriságát.

kockázatkezelés: Védelmi intézkedések kidolgozása, elemzése és meghozatala, amelyet követően a maradványkockázatok elviselhető szintűre változnak.

kockázatarányos védelem: az a védelem, mely a kockázatokat a releváns fenyegetettségek bekövetkezési valószínűsége és a fenyegetettség bekövetkezésekor keletkező kár függvényeként kezeli, és ahol a védelemre fordított erőforrások értéke arányos a védendő értékek nagyságával, illetve kockázatcsökkentő képességével.

kötelező hozzáférés-védelem: A szubjektumokhoz, és az objektumokhoz egy jelző (címke) van rendelve, azok titokvédelmi osztályozása szerint A hozzáférés akkor engedélyezhető, ha a szubjektum titokvédelmi osztályozása uralkodik az objektum titokvédelmi osztályozása felett.

közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső adat;

közérdekből nyilvános adat: minden olyan, természetes személy, jogi személy vagy jogi személyiséggel nem rendelkező szervezet kezelésében lévő vagy rá vonatkozó, a közérdekű adat fogalma alá nem tartozó adat, amelynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

központi mentés: Az a mentési eljárást, amikor egy hálózatos rendszerben a szétszórt, vagy a hálózat egy-egy csomó-pontjában található adatokat egy kijelölt csomóponti számítógépen tárolják, vagy erre átmozgatják, és ezen a számítógépen készül a mentés.

különleges adat:
a) a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra,

b) az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat;

legális szoftver: Az a szerzői jog védelme alatt álló szoftvertermék, amelynek legalitásának igazolásához minden szükséges dokumentum (licence, számla, szállítólevél, ajándékozási szerződés stb.) rendelkezésre áll, valamint a használata a szoftver licence szerződés előírásainak megfelelő módon történik.

logikai bomba: A vírus olyan része, illetve szerkezete, amelyik időhöz, esemény bekövetkezéséhez, logikai változó adott értékéhez kötött módon aktivizálódik.

logikai védelem: Az informatikai rendszerekben informatikai eszközökkel megvalósított védelem.

mentés, mentési rend: Az alkalmazás (tágabb értelemben az informatikai rendszer) egy-egy környezetének (tehát nem csak adattartalmának) alkalmas hordozóra történő másolása a mentett környezet épségének megbontása nélkül. A mentés általában biztonsági érdekből, a mentett környezet visszaállításának céljával készül. A mentési rend a mentett környezet elemeinek meghatározásából, a mentés körülményeinek előírásából áll, ide sorolva a mentett környezet állapotának megszabását, a mentés időpontjának- vagy idő-szakának előírását, a mentés periodicitásának megszabását, kezelési / őrzési / tárolási előírásokat, a tárolási helyre vonatkozó előírásokat, az alkalmazandó jelzéseket/nyilvántartásokat, frissítési szabályokat, stb. A mentési utasítás célja a későbbi sikeres felhasználás/visszaállítás garantálása.

maradványkockázat: Az tudatosan felvállalt kockázat, amely alapvetően – kis mértékben – annak ellenére is fennmarad, hogy a fenyegető tényezők ellen intézkedések eredményesen végrehajtásra kerültek.

megbízható működés: Az informatikai rendszerek, és az általuk kezelt adatok által hordozott információk rendelkezésre állásának és funkcionalitásának védelme.

megbízhatóság: A megbízhatóság műszaki értelemben egy informatikai rendszerelemnek vagy rendszernek az a jellemzője, amely megadja, hogy az üzemeltetési feltételek fenntartása esetén milyen mértékben várható el annak hibátlan, rendeltetésszerű működése.
A megbízhatóság matematikai értelemben egy statisztikai fogalom, amely annak a valószínűségét adja meg, hogy egy rendszerelem, vagy rendszer jellemzői az előírt határok közé esnek.

meghibásodási tényező: Az informatikai rendszer (vagy rendszerelemek) megbízhatóságát jellemző olyan mutatószám, amely megadja, hogy adott időpont után, kis időegységen belül, az informatikai rendszerelemnek mekkora a meghibásodás valószínűsége, feltéve, hogy az adott időpontig az eszköz nem hibásodott meg.

meghibásodások közötti átlagos működési idő: Az informatikai rendszerek megbízhatóságának jellemzésére gyakran használt mennyiségi mutató, a két egymást követő meghibásodás közötti hibátlan működés átlagos ideje.

meg nem kerülhetőség: Annak biztosítása, hogy egy védelmi intézkedést nem lehet más úton kijátszani.

mentés: Az az informatikai folyamat, amelynek során az informatikai rendszerben digitálisan tárolt, vagy használatban lévő fontos adathalmazokról egy speciális eszközzel egy speciális adathordozóra (mentési médium) másolatokat készítenek.

mentési médium: Az az adathordozó (a legtöbbször mágneses elven működő szalagos egység), amelyen a mentések által duplikált adattartalmat tárolják.

mentő eszköz: Minden olyan informatikai berendezés, amely segítségével az informatikai rendszerben meglévő adatbázisokról elektronikus másolat készíthető.

mentő szoftver: Olyan szoftver, amely az operációs rendszer és a mentő eszköz közötti kapcsolatért felelős, továbbá ennek a feladata biztosítani, hogy az adatbázis duplikációját speciális körülmények között is el lehessen a mentési médiumra készíteni.

minősítés: Az a döntés, amelynek meghozatala során az arra felhatalmazott személy megállapítja, hogy egy adat a tartalmánál fogva a nyilvánosságát korlátozó titokkörbe tartozik.

működőképesség: A rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fennmaradása. A működőképesség fogalom sok esetben azonos az üzembiztonság fogalommal. Ezen állapot fenntartásának alapfeladatait a rendszeradminisztrátor (rendszergazda) látja el.

működési zavar, rendkívüli esemény: Az IT rendszer működési folyamatában beálló rendellenesség, szabálytalanság. Eltérés a rendeltetésszerű működéstől.

naplózás: A felhasználói jogosultságok rögzítésére, dokumentálására szolgáló, és a számonkérést biztosító funkció a hozzáférés-védelemben.

Nyilvános Kulcsú Infrastruktúra: A Hitelesítés Szolgáltatónak nemzetközi feltételeket, szabványokat kielégítő biztonságos rejtjelzési módszereit, a személyzetre, a fizikai és az informatikai környezetre kiterjesztő infrastruktúrája.

Nyilvános kulcsú rendszer: Olyan kriptográfiai rendszer, amelynek a résztvevői közös algoritmust használnak, a rejt jelzésre és a megoldásra. A rejt jelző algoritmusnak két – a használótól függő – kulcsa van. Ezek egyikét (nyilvános kulcs) a nevükkel együtt nyilvánosságra hozzák, a másikat pedig titokban tartják (titkos kulcs). A kulcsok egyikét a rejt jelzésre, a másikat a megoldásra használják.

nyilvánosságra hozatal: Az adatnak meghatározhatatlan körben, mindenki részére biztosított megismerhetővé, hozzáférhetővé tétele;

PKI: Public Key Infrastructure (lásd *Nyilvános Kulcsú Infrastruktúra*).

probléma: Olyan egyedi, jelentős hatású zavaró esemény, amely hatása nagymértékben rontja a felhasználók számára nyújtott informatikai szolgáltatás minőségét.

rendelkezésre állás: Az informatikai rendszer tényleges állapota, amely megvalósul, ha a rendszer szolgáltatásai állandóan, illetve egy meghatározott időben hozzáférhetők és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

rendszer: Az egymással valamilyen meghatározható kapcsolatban álló elemek összessége.

rendszerelemek: Az adatokat „körülvevő", az informatikai rendszer részét képező elemek.
rendszerprogram (rendszerszoftver): Olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardverei használhatók legyenek és az alkalmazói programok működjenek. (A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.)

rendszergazda (adminisztrátor): az a szervezeti egység vagy személy, amely vagy aki az adott rendszer üzleti elvárás szerinti működtetéséért felelős.
Az informatikai rendszerekben teljes, vagy kiemelt jogosultságokkal rendelkező felhasználó, aki az informatikai rendszerrel kapcsolatos napi üzemeltetési feladatokat ellátja, beleértve a hozzáférési jogosultságokkal kapcsolatos tevékenységeket, többek között a számítógépek és a rajtuk lévő felhasználói fiókok és csoportok telepítését, beállítását, kezelését végezheti

rendszer leírás: célszerűen használható, de nem pontos összefoglaló fogalom, amely a pénzügyi jellegű rendeltetésű alkalmazás (informatikai rendszer) vagy az ezekhez tartozó rendszerelem dokumentációját jelöli. A pontos megjelölés a pénzügyi intézmény (vagy alkalmazás szolgáltató vagy alkalmazás szállító) belső ellenőrzési rendszerében előírt, szabványos specifikáció, rendszer/modul terv, fejlesztési dokumentum, tesztelési jegyzőkönyv, üzemeltetési utasítás, felhasználói utasítás, stb. lenne.

Shareware szoftver: Időszakosan ingyenesen használható szoftver. Korlátozott funkcionalitás, regisztrálási illetve fizetési kötelezettség jellemzi.

számonkérhetőség: Annak biztosítása, hogy az informatikai rendszerben végrehajtott tevékenységek a későbbi ellen-őrizhetőség céljára rögzítésre kerüljenek.

számítástechnikai adathordozó: számítástechnikai eljárással adatokat rögzítő, tároló adathordozó (mágnesszalag, hajlékony és merevlemez, CD stb.), amely az adatok nyilvántartását, azonosítását, kezelését és visszakeresését biztosítja.

személyes adat: bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: **érintett**) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet;

személyesadat-nyilvántartó rendszer (nyilvántartó rendszer): személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető;

szervezeti és működési szabályzat: a Hivatal tevékenységének alapdokumentuma, amely rögzíti a szerv, azon belül a szervezeti egység feladatait és a feladatokhoz rendelt hatásköröket.

szoftver: Valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.

szoftvergazdálkodás alapelvei: A szoftverbeszerzés és terítés alapvető elemei, mint például a következők: 1., Kizárólag legális (jogtiszta) szoftvereket lehet használni. 2., Csak azokat a szoftvereket szabad a számítógépekre telepíteni, amelyek a munkavégzéshez feltétlenül szükségesek. 3., Minden dolgozó számára biztosítani kell a munkája hatékony és eredményes elvégzéséhez szükséges szoftverkörnyezetet. 4., Egységesség, a konfigurációk könnyű menedzselhetősége.

szoftverleltár: Annak dokumentált leírása, hogy az intézmény informatikai rendszerébe tartozó minden egyes számítógépen és szoftver futtatására alkalmas eszközön milyen szoftverek találhatók.

szükséges tudás elve: Az érzékeny információ tulajdonosa részéről az információk elérésére, birtoklására, és azokon tevékenység végrehajtására vonatkozó jogosultságok meghatározása egy felhasználó részére, annak hivatali kötelezettségei függvényében.

teszt (rendszer) környezet: Az alkalmazás szolgáltató szervezet/cég informatikai rendszerébe tartozó mindazon komponensek összessége, amelyet egy adott pénzügyi jellegű rendeltetésű alkalmazás ellenőrzése érdekében állítanak össze. Teszt környezet érvényes eredményt/tranzakciót előállító módon nem működhet.

teljes körű védelem: Teljes körűnek nevezik az informatikai rendszer védelmét, ha az informatikai rendszer összes elemére kiterjed.

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

titokvédelem: Az adatvédelem körébe tartozó adatok, és az egyéb erőforrások bizalmasságának védelmi körülményeinek megteremtése.

titkos személyi információk: Minden olyan, az egyes ügyfelekről az intézmény rendelkezésére álló tény, információ vagy adat, amely az ügyfél személyére, adataira, vagyoni és pénzügyi helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi és/vagy üzleti kapcsolataira, valamint az adott intézménnyel fennálló kapcsolatára vonatkozik.

trójai program: Olyan rosszindulatú programtörzs, amelyeket készítője illegálisan épített be az általa tervezett programba és a felhasználó szándéka ellenére és tudta nélkül hajt végre illegális feladatokat (pl.: adattörlés, illegális lemezművelet, program-megsemmisítés stb.).

tűzfal: Egy olyan számítástechnikai eszköz, amely fizikailag, és logikailag elválaszt egy hálózatot egy másiktól.

ügyfél: az a személy, aki a szolgáltatóval a szolgáltató tevékenységi körébe tartozó szolgáltatás igénybe vételére szerződést köt (rendszeres ügyfél), illetve a szolgáltató részére ügyleti megbízást ad (alkalmi ügyfél)

üzleti titok: a Hivatal tevékenységéhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek a titokban maradásához a Hivatalnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a szükséges intézkedéseket megteszi.

visszatöltés: Az a folyamat, amelynek során a mentett adatokat tartalmazó médiumról a mentő eszköz segítségével a sérült adathalmaz utolsó ép állapotának leginkább megfelelő adatstruktúrát visszaállítják.

vírus: Olyan rosszindulatú programtörzs, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet, "megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói programot, sokszorozva önmagát (ami lehet mutáns is) és a logikai bomba hatás révén egy beépített feltételhez kötötten (pl.: konkrét időpont, szabad lemezterületi helyek száma stb.) trójai faló hatást indít el.

vírusvédelmi rendszer: A vírusvédelmi rendszer és a hozzá kapcsolódó védelmi mechanizmusok feladata az informatikai rendszerhez kapcsolódó vírusok felkutatása, működésük, aktív vagy passzív károkozásuk megakadályozása, illetve – lehetőség szerint – megsemmisítésük.

„B" Melléklet - Az Internet használatára vonatkozó biztonsági standardok

Az Internet használata során a Hivatal fenntartja a jogot arra, hogy a felhasználók Internet-forgalmát figyelje, illetve naplózza. A felhasználók tudomásul veszik, hogy az általuk látogatott oldalakra vonatkozó információkat a Hivatal ilyen módon kezeli, és ennek elfogadásáról írásban nyilatkoznak. A felhasználók által leggyakrabban látogatott weboldalakat a Hivatal adatvédelmi felelőse szúrópróbaszerűen megvizsgálja.

Interneten keresztül elsősorban a munkavégzéshez szükséges szakmai információk beszerzése történhet!

Minden alkalmazottnak ügyelnie kell arra, hogy a Hivatal hálózatán keresztül személyes Internet-használatot minimális szinten tartsa (ideértve a munkaidőn túli Internet használatot is).

Az Internet használata során követendő magatartás:

Az alkalmazottak nem titkolhatják el személyazonosságukat az Internet használata közben. Az Internet használatakor az alkalmazottaknak egyértelműen azonosítaniuk kell magukat.

A Hivatal munkavállalói nem hirdethetik, nem jeleníthetik meg, és semmi más módon nem nyilváníthatják ki véleményüket az Internet-fórumokon (pl. levelezőlista, vitafórum, chat fórum, stb.) a Hivatal szolgáltatásaival kapcsolatban az aljegyző jóváhagyása nélkül.

A szellemi tulajdon védelme az Internetre is kiterjed. Az Internet jelenlegi jogi szabályozatlansága könnyen lehetőséget ad a szellemi tulajdonnal összefüggő jogi problémák kialakulására.

Csak megfelelő vezetői engedéllyel tölthetnek át a felhasználók harmadik féltől licenszelt vagy a Hivatal által (megrendelésére) fejlesztett szoftvereket más gépre az Interneten keresztül.

Bármilyen letöltés csak informatikusi vagy vezetői engedéllyel lehetséges.

Az Internet hozzáféréssel rendelkező munkatársak nem használhatják a Hivatal Internet-kapcsolatát szórakoztató szoftverek, vagy játékok letöltésére, valamint Internetes játékokra. Egyes weboldalak elérhetőségét a Hivatal nem teszi elérhetővé munkatársai számára. Ennek ellenőrzése szúrópróbaszerűen történik.

Intézkedések betörések esetére

Behatolási kísérlet esetén ki kell deríteni, hogy ki próbált behatolni, és meg kell határozni a behatolási felületeket. Sikeres betörés esetén elsőrendű feladat a tűzfal konfiguráció kijavítása, hogy a belső hálózat biztonsága megteremtődjék. Szükséghelyzetben az intézkedések az egyedi hozzáférési lehetőség megszüntetéséig, bizonyos számítógépek kikapcsolásáig, illetve az Internet kijárat megszüntetéséig is kiterjedhetnek. Minden eseményt naplózni kell és minden bizonyítékot fel kell használni, hogy a behatoló követése és azonosítása lehetővé váljon.

Behatolások detektálása

A behatolások hatékony detektálására legalább a hálózat nyilvános külső kapcsolatainak forgalmát valósidejű behatolás-detektáló rendszerrel kell védeni. Minden behatolási kísérletet naplózni kell, ezeket a naplókat az esemény kivizsgálásának befejezéséig meg kell őrizni. Minden behatolási kísérletet azonnal, riasztással jelezni kell az Informatikai Biztonsági felelősnek, a kijelölt rendszergazdának, vagy az informatikusnak.

A védelem hatékonyságának megőrzése érdekében a rendszert folyamatosan naprakészen kell tartani. A rendszer konfigurációs állományait nem módosítható adathordozón, biztonságosan elzárva is tárolni kell.

A behatolás-detektáló rendszert használni kell legalább az Internetre kötött hálózati eszközök és a lokális hálózat forgalmának ellenőrzésére.

„C" Melléklet - Az Elektronikus levelezésre vonatkozó biztonsági standardok

A felhasználók igénybe vehetnek elektronikus levelezési szolgáltatást. A postafiók címet minden felhasználónál a következőképpen képezzük:

vezetéknév.keresztnév@budavar.hu

keresztnév.vezetéknév@budavar.hu

Az elektronikus postafiókcím nem tartalmaz ékezetes karaktereket. A levelek lekérdezéséhez csak és kizárólag a Microsoft Outlook levelezőprogramját lehet és kell használni.

E-mailen keresztül elsősorban a munkavégzéshez szükséges szakmai információk fogadása és küldése történhet, a szervezeti egység vezetőjével egyeztetett módon.

A felhasználók kötelesek minden munkakezdéskor és napközben rendszeresen ellenőrizni e-mail üzeneteiket.

Az e-mail üzenetek nem tartalmazhatnak meghatározott kiterjesztésű fájlokat, melyek a következők: *.bat, *.com, *.exe, *.js, *.pif, *.scr, *.vbe, *.vbs. és egyéb futtatható alkalmazások (kisalkalmazások) kiterjesztései.

A technológiai fejlődés kapcsán a kizárható fájlok felülvizsgálatát a rendszeres vírusvédelmi hírlevelek alapján meg kell tenni.

A rendszernek automatikusan vissza kell utasítania a levelet, ha az mégis tartalmazza a fent említett kiterjesztésű fájlok valamelyikét.

Az üzenet és a hozzá tartozó csatolások maximális mérete nem haladhatja meg a 10 Mbyte -ot!

Amennyiben az üzenet mérete nagyobb, a rendszer nem kézbesíti a levelet, és erről értesíti a feladót.

A szerveren tárolt postafiók mérete (kvóta) 100Mbyte lehet. Ennek megközelítésekor a felhasználó automatikus figyelmeztetést kap. Ha a fenti kvótát meghaladja, a postafiók mérete a szerver a levélforgalmazást az adott felhasználónál korlátozza, és értesítést küld az informatikusnak.

Minden felhasználónak tilos a Hivatal nevében olyan e-mailt küldeniük, csatolt fájlt megjeleníteni mely:

- bizalmas, kritikus és kereskedelmi szempontból érzékeny információt tartalmaz,
- a Hivatal hírnevét, vagy üzletfeleivel való kapcsolatát negatív irányban befolyásolhatja,
- a Hivatal üzletfeleinek adatbiztonságát sértheti
- Vírusokkal fertőzhet meg bármely Hivatali hálózatot vagy üzletfelek hálózatát.
- tilos ún. lánclevelet továbbítani, ezzel ugyanis a cég levélszemét küldő (SPAM) listára kerülhet, mely lebéníthatja a levélforgalmat.

Szakmai ügyekkel kapcsolatos e-mail üzeneteket a címzettnek ki kell nyomtatnia, és a központi iktatóba iratkezelésre be kell adnia, majd a vonatkozó levelezésben le kell fűznie.

A munkavégzéssel kapcsolatosan már nem használható leveleket a felhasználók rendszeresen kötelesek eltávolítani postaládájukból.

„D" Melléklet - Számítógépes vírusokra vonatkozó biztonsági standardok

Célja:

A Hivatal hálózatában használt számítógépek és a rajtuk tárolt adatok megvédése az ártalmas vírusokkal szemben.

Érvényességi területe:

A Hivatal informatikai hálózata

A védelemhez használt szoftverek:

- kliensek, windows szerverek védelme (jelenleg Kaspersky végpont felügyelet –KES)
- Levelezés -Mail Gateway védelem(email átjáró vedelme- jelenleg Kaspersky Exchange Security)

A vírusminták a napi frissítés miatt változó verziójúak!

Vírusok bejutásának kockázata:

- Internetről (bérelt vonali összeköttetésű hálózat),

- E-Mail rendszeren keresztül,

- Adathordozóval (pendrive, CD, egyéb)

Védekezés.

Vírusminták frissítése

Az vírusvédelmi alkalmazásokat futtató szerveren a Kaspersky Security Center(KSC)menedzsment modul minden nap legalább egyszer letölti a definíciós mintát, majd küldi szét a bekapcsolt munkaállomásoknak, szervereknek. Amennyiben a munkaállomás nem volt bekapcsolva, úgy a következő bekapcsoláskor töltődik le rá a minta.

Szerverek:

- Az összes kimenő és bejövő file vizsgálata,
- Vírus esetén törlés
- Jelzés a felhasználónak a vírus jelenlétéről és a vírusmentesítés eredményéről egy „popup" üzeneten keresztül, ill. bejegyzés az esemény naplóba.

Munkaállomások:

- Az összes kimenő és bejövő file vizsgálata
- Vírus esetén törlés, karanténba helyezés
- Jelzés a felhasználónak a vírus jelenlétéről és a vírusmentesítés eredményéről egy „popup" üzeneten keresztül, ill. bejegyzés az esemény naplóba.

Exchange (levelező és csoport munka) szerver:

- Az összes kimenő és bejövő levél vizsgálata
- Több kötetes tömörített file-ok és jelszóval védett file-ok nem továbbíthatóak (program nem tudja biztonságosan leellenőrizni)
- Vírus esetén csatolt file törlése, figyelmeztető levél küldése a feladónak és a címzettnek.

Kaspersky Exchange Security a levelező szerveren:

- Az összes kimenő és bejövő levél vizsgálata

- Az összes kimenő és bejövő levél SPAM szűrése
- Vírus esetén csatolt file törlése, figyelmeztető levél küldése a feladónak és a címzettnek.

Vírus vagy illetéktelen behatolási kísérlet észlelésekor a külső kapcsolatot azonnal meg kell szüntetni (böngészőt, levelező klienst lezárni). A kapcsolat megszűnésével a munkaállomást a rendszergazda fizikailag leválasztja a külső kapcsolódási pontról és belső hálózatról. A munkaállomás belső hálózatra történő visszahelyezése vírusmentesítés után lehetséges.

Nem Hivatali tulajdonú bármilyen adathordozó bármelyik számítógépbe (munkaállomás, szerver) helyezése karantén (nem hálózatra kapcsolt) gépen történő vírusellenőrzés után lehetséges. A vírusellenőrzést, vírusmentesítést informatikus végzi. Beszállítótól, szolgáltatótól érkező adathordozó vírusmentességét a beszállítóknak kell garantálnia, de a vírusellenőrzést ebben az esetben is kötelező végrehajtani.

A felhasználók kötelesek azonnal jelenteni az informatikusnak, ha számítógépes vírus jelenlétére utaló jelet fedeznek fel (pld. a telepített Kaspersky vírusirtó program biztonsági figyelmeztetést küld.).

„E" Melléklet - Nyilatkozat az informatikai eszközök és szolgáltatások használatáról

Alulírott, _____ kijelentem, hogy a Budapest Főváros I. kerület Budavári Polgármesteri Hivatala (továbbiakban Hivatal) Informatikai Biztonsági Szabályzatát ismerem, az abban foglaltakat tudomásul veszem, és magamra nézve kötelezőnek fogadom el, azt betartom.

Kijelentem, hogy a Hivatal Internet szolgáltatásokkal kapcsolatos mindenkor hatályos szabályzatait, szabályait megismertem, az abban foglaltakat tudomásul veszem, magamra nézve kötelezőnek fogadom el. Tudomásul veszem, hogy a Hivatal az Internet hozzáférést, valamint az elektronikus levelezést csak üzleti céllal bocsátja rendelkezésemre, és jogosult annak forgalmát folyamatosan figyelni.

Kijelentem továbbá, hogy a személyes használatomra a Hivatal által biztosított számítógépes munkahelyen telepített szoftver komponensek, programok listáját ismerem és ezeken felül semmilyen új komponenst, adatot vagy programot az informatikus és az üzemeltetést ellátó szolgáltató hozzájárulása nélkül feltelepíteni nem fogok.

Tudomásul veszem, hogy minden olyan kárért és veszteségért, amely a személyi számítógépemre telepített, de nem engedélyezett komponensek következtében áll elő anyagi és büntetőjogi felelősséggel tartozom.

Tudomásul veszem, hogy a Hivatal az Informatikai Biztonsági és Adatvédelmi Szabályok betartását bármikor jogosult ellenőrizni.

Budapest, ...

.....
Aláírás

- **„F" Melléklet- Változáskezelési lap**

A Benyújtó tölti ki:

Benyújtó neve:	
Beosztása:	
Elérhetősége:	
e-mail:	
telefon:	
Benyújtás dátuma:	
Aláírás:	

A változtatni kívánt dokumentum neve, fejezet és/vagy bekezdés száma, megnevezése:

A változtatás rövid indoklása:

A javasolt új szövegrész:

IT Szolgáltatásmenedzser tölti ki

Beérkezés időpontja:	
Átvevő:	

Az igény vizsgálatával kapcsolatos megjegyzések:

Az igény elbírálása: Bekerül a dokumentumba a változtatás

NEM kerül be a dokumentumba a változtatás

Indoklás:

Aláírás:

- **„G" Melléklet- Titoktartási nyilatkozat**

Alulírott ....., az ..... dolgozója kijelentem, hogy a BUDAPEST FŐVÁROS I. KERÜLET BUDAVÁRI POLGÁRMESTERI HIVATAL (továbbiakban: Megbízó) által rám bízott, vagy a munkám során tudomására jutott üzleti titkot, (a gazdasági tevékenységhez kapcsolódó minden olyan tényt, információt, megoldást vagy adatot, amelynek nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a jogosult jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné), valamint a Megbízóra, illetve a tevékenységére vonatkozó alapvető fontosságú információkat:

- Bizalmasan kezelek,
- Azokat harmadik személynek át nem adom,
- Azokról harmadik személynek (és/vagy a médiának) nyilatkozatot az adatok tulajdonosának dokumentált engedélye nélkül nem teszek,
- Magam, vagy mások hasznára azok részeit, vagy egészét hasznosítás céljából nem alkalmazom.

Amennyiben, az integrált informatikai rendszer beszerzésére vonatkozó megállapodás nem jön létre, az átadott adatokat megsemmisítem, és erről a Megbízónak írásban nyilatkozom. .

Tudomásul veszem, hogy a titoktartási kötelezettség megszegése esetén a Polgári Törvénykönyvben meghatározott jogkövetkezmények alkalmazhatóak velem szemben.

Budapest, 2017.....

.....

aláírás

- **„H" Melléklet- A Elektronikus Információs Rendszerek besorolása**

Az informatikai rendszer megnevezése	Az informatikai rendszer leírása	Adatgazda	B	S	R	Az informatikai rendszer biztonsági osztálya
Hagyaték	Hagyatéki nyilvántartó rendszer	Szarka Lászlóné Igazgatási ügyintéző 458-3002	2	2	2	2
ALFA_MAP	Közműnyilvántartó	Holló Marianna városüzemeltetési ügyintéző 458-3071	2	2	1	2
DMS	Elektronikus iktató rendszer	Hergár Péter IT szolgáltatás manager 458-3043	2	2	1	2
EPER	Gazdasági szakrendszer	Hordos Andrea Gazdasági irodavezető 458-3023	2	2	1	2
GISPAN	Ingatlan és vagyonkataszter	Szeleczky Szilvia Műszaki irodavezető 458-3027	2	2	1	2
ÖNKADÓ	Kerületben alkalmazott adónemeket tartalmazó nyilvántartó program	Melovics József Adóügyi csoportvezető 458-3026	2	2	2	2
Govcenter	Kereskedők nyilvántartása - kiskereskedelem, vendéglátó, szálloda	Dr. Botár Ildikó Tünde Igazgatási irodavezető 458-3021	2	2	1	2
SZOCINFO	Szociális információs rendszer	Fábik Gabriella szociálpolitikai ügyintéző 458-3033	2	2	2	2
Levelezés	Elektronikus levelezés	Hergár Péter IT szolgáltatás manager 458-3043	2	2	1	2
Fájl szerver	Fájlok tárolása	Hergár Péter IT szolgáltatás manager 458-3043	2	2	1	2

- „I" Melléklet- Jogosultság Igénylő Lap(JIL)

HOZZÁFÉRÉSI JOGOSULTSÁG KÉRŐ ADATLAP

A köztisztviselő	
Neve	
Jogviszony típusa (közszolgálati, közalkalmazotti, szerződéses, stb)	
Beosztása	
A hivatali szervezeti egysége	
Szervezeti egység vezetője	
Közvetlen vezetője (csoportvezető)	
Jogviszony kezdete/vége	
Munkavégzés helye (cím, emelet, ajtó)	Budapest, Kapisztrán tér 1. I.em.112.

Alkalmazás igénylés *(X-el jelölje)*	
Irodai programcsomag (MS Office)	
Iktató	
Levelezési postafiók	
Internet	
Pénzügyi rendszer	
Egyéb alkalmazás:	

Iratkezelő rendszer jogosultsága (X-el jelölje a megfelelőt)	
iktató, iratkezelő(Kulcsfelhasználó)	
szignáló (vezető)	
Ügyintéző	
Dátum: 20....év .....hó .....naptól. - 20....év .....hó .....napig.	

Kérjük, hogy kitöltés után a nyomtatványt aláírva a Jegyzői Referatúrára szíveskedjen eljuttatni.

Budapest, 201.....

szervezeti egység vezetője személyügyi ügyintéző

„J" Melléklet- Karbantartási napló

Karbantartási Napló

Karbantartott eszköz neve:

Érintett rendszer:

Karbantartás típusa: Tervezett/rendkívüli

Karbantartás indoka:

Elvégzett tevékenység:

Várható leállás dátuma:

Leállás valós dátuma:

Leállás tervezett időtartama:

Leállás tényleges időtartama:

Karbantartás eredménye:

Megjegyzés

Dátum:

Karbantartó neve: