CERTIQUA Minőségügyi és Informatikai Tanácsadó Bt. • 9700 Szombathely, Csillag u. 21.
Telefon: 20/464-4458 • 20/399-0678 • Email: info@certiqua.hu • Web: www.certiqua.hu

Bükiné

RÉPCELAK VÁROS ÖNKORMÁNYZATÁNAK

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

2006. DECEMBER

DOKUMENTÁCIÓ VERZIÓJA: 1.0

Hatályos: 2007. január 1-től.

Tartalomjegyzék

I.
Általános rész

Répcelak Város Polgármesteri Hivatal (továbbiakban Hivatal), mint adatkezelő köteles gondoskodni a hatályos jogszabályokban és belső utasításokban előírt informatikai védelmi követelmények tejesítéséhez szükséges technikai és szervezési feltételek biztosításáról, valamint az adatkezelés biztonságát szolgáló eljárási szabályok kiadásáról és betartásáról.

Az informatikai védelem a következőket foglalja magába:

- a működéshez szükséges információk alaposságának, pontosságának, teljességének, törvényességének és sértetlenségének biztosítását;
- a szükséges adatok megóvását a jogosulatlan kezelésektől és manipulációktól: hozzáférés, módosítás, törlés, megsemmisítés, átadás;
- a Hivatal dolgozóinak az adatkezelés körében gondatlanul vagy szándékosan elkövetett illetéktelen beavatkozásától és mindennemű „külső" beavatkozástól történő védelmét;
- a számítástechnikai alkalmazási rendszerek, berendezések, hálózati eszközök biztonságának elősegítését.

II.
Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat (továbbiakban: Szabályzat) célja, hogy a Hivatal szervezeti egységeinél az informatikai rendszerek alkalmazása és karbantartása során lehetővé tegye a kezelt adatok használati és tárolási biztonságát.

A Szabályzat alkalmazása kiterjed a hivatali és a hivatali rendszerekhez kapcsolódó informatikai rendszerek alkalmazásának teljes időtartamára, a beszerzések tervezésére, az üzemeltetésre, az adatfelhasználásra, az adatátadásra valamint az eszköz- és adatmegsemmisítésre egyaránt.

A Szabályzat alkalmazása során biztosítani kell:

- az üzemeltetett informatikai rendszerek és infrastruktúra rendeltetésszerű használatát, zavartalan üzemeltetését és az üzembiztonságot szolgáló karbantartást;
- az informatikai rendszer üzemeltetési folyamatára, az információtárolás és feldolgozás minden elemére az illetéktelen felhasználás kizárását;
- illetéktelen szoftverek alkalmazásának kizárását;
- az informatikai eszközök, az alkalmazott szoftverek, az adatok, az adatállományok és beállítási paraméterek (egyedi jelszavak, hálózati alkalmazási paraméterek) tartalmi és formai épségét, megfelelő tárolását és annak védelmét;
- a szoftverek és az adatállományok dokumentációinak meglétét és megőrzését;
- az alkalmazott informatikai eszközök és az egységes informatikai hálózat megléte esetén annak dokumentációinak nyilvántartását és megőrzését;
- az információtárolás és -feldolgozás folyamatát fenyegető veszélyek megelőzését és elhárítását;

- a védelem működését a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig;
- a titok-, vagyon- és tűzvédelemre vonatkozó előírások (törvények, szabályzatok, rendeletek, utasítások) betartását;
- a speciális adatvédelmi szabályzatok (pl. Közszolgálati Nyilvántartás stb.) előírásainak betartását és jelen Szabályzattal összhangban történő alkalmazását.

III.
Általános rendelkezések

3.1. A Szabályzat hatálya

Személyi hatály
A Szabályzat személyi hatálya kiterjed a Hivatal valamennyi dolgozójára, az informatikai eljárásokban részt vevő más szervezetek dolgozóira (pl. hálózat- és számítógép-javítást, -karbantartást, szoftvertelepítést és -karbantartást végző szakemberekre), valamint azokra, akik kapcsolatba kerülhetnek a Hivatal informatikai rendszerével (takarító, festő, általános karbantartó, stb.)

A Szabályzat előírásait kell alkalmazni a Hivatal kezelésében lévő adatok felvétele, feldolgozása, módosítása, tárolása, a Hivatalon belüli és külső szervezetek részére történő átadása, hasznosítása és nyilvánosságra hozatala alkalmával egyaránt.
A Szabályzat előírásai vonatkoznak mindazokra, akik az adatokba betekinthetnek, az adatok hozzáféréséhez engedélyt adnak és az adatfeldolgozás technikai feltételeit biztosítják.
A Szabályzat előírásainak betartása minden dolgozó feladata és személyesen felel az adatok védelmének biztosításáért.

A kezelt adatok köre az alábbiakra terjed ki:
- a szervezeti egységeknél feladataik ellátása során keletkezett és kezelt adatok;
- más szervezeti egységektől kapott adatok;
- azon adatok, amelyekre betekintési vagy felhasználási jogosultságot kaptak;
- minden olyan adat, amely a feladataik elvégzéséhez közvetlenül nem szükséges, de a különböző hivatali információs csatornákon tudomást szereztek róla.

Tárgyi hatály
A Szabályzat tárgyi hatálya kiterjed:
- a védelmet igénylő adatok teljes körére, felvételük módjától, valamint feldolgozási eredményüktől, -helyüktől, -idejüktől és fizikai megjelenési formájuktól függetlenül;
- a Hivatal alkalmazásában lévő valamennyi (saját és idegen tulajdonú) informatikai eszközre, berendezésre és azok műszaki dokumentációjára;
- az adatfeldolgozási és egyéb informatikai folyamatokban szereplő valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési);
- a rendszer-, a felhasználói- és az általános nyilvántartási szoftverekre;
- az adatok felhasználására, tárolására vonatkozó utasításokra;
- az adathordozók alkalmazásba vételére, használatára, tárolására és megsemmisítésére.

3.2. A Szabályzat minősítése

A Szabályzat a Hivatal belső használatára szolgáló, publikus minősítésű dokumentum.
Az intézmény az általa kezelt adatok biztonsági osztályba sorolása alapján „Információ-védelmi alapbiztonsági (IV-A) osztály" biztonsági besorolásba tartozik.

3.3. A Szabályzat érvényessége

A Hivatal Informatikai Biztonsági Szabályzatának kiadása: **2006. november 30.**
A Szabályzat visszavonásig érvényes.

3.4. Értelmező rendelkezések, műszaki alapfogalmak

Adat: valamilyen dolog, esemény, állapot jellemzőinek leírására és azok rögzítésére szolgáló eszköz, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája. Informatikai rendszereken belül az információk kódolva, adatok formájában fordulnak elő. Ahhoz, hogy az informatikai rendszerben tárolt adatokat érthetővé tegyük, át kell alakítani, interpretálni vagy magyarázni kell azokat.

Adatállomány/adatbázis: az információk elektronikus tárolását lehetővé tevő, adatokkal feltöltött adatstruktúra, melyet névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz.

Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki, technikai és szervezési intézkedések és eljárások együttes rendszere.

Adathordozó: az információk elektronikus úton történő rögzítésére, tárolására és átadására használható eszköz:

- mágneslemez,
- beépített/hordozható merevlemez,
- CD/DVD lemez,
- mágnesszalag,

Adathordozóként alkalmazzuk az informatikai eszközök összekapcsolásából kialakított Internet, Intranet és Externet hálózatokat is.

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 jogszerűségére vonatkozik.
Bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

Hálózat: két vagy több számítógép összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé.

Hitelesség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

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

Informatikai biztonság: A biztonság egyszerre jelenti a rendszer működőképességét, rendelkezésre állását, az információk bizalmasságát, hitelességét és sértetlenségét. A biztosság az a kedvező állapot, amelynek megváltozása nem valószínű, de nem is lehet kizárni. Vagyis minél kisebb a változás valószínűsége, annál nagyobb a biztonság. Az informatikai biztonság a védeni kívánt informatikai rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely az informatikai rendszerekben kezelt adatok zárt, teljes körű, folytonos és a kockázatokkal arányos védelmét valósítja meg.

Informatikai eszköz: számítógép, terminál, monitor, nyomtató, kiegészítő eszköz (egér, klaviatúra, kamera, mikrofon, stb.), adatátviteli eszköz (Hub, Switch, modem, adatátviteli hálózati végpont, stb.).

Informatikai rendszer: az információ rögzítését, tárolását, módosítását, feldolgozását és továbbítását lehetővé tevő informatikai eszközök és szoftverek kombinációjából álló rendszer. Az informatikai rendszerek különleges tulajdonsága a szabad programozhatóság.

Információ: valamilyen dolog, esemény, állapot leírására szolgáló közlés, tájékoztatás, hír eddig ismeretlen adattartalma. Jelentéssel bíró szimbólumok összessége, amelyek jelentést hordozó adatokat tartalmaznak és olyan új ismeretet szolgáltatnak a megismerő számára, hogy ezáltal annak valamilyen bizonytalanságát megszüntetik és célirányos cselekvését kiváltják.
Az információ általános értelemben a valóság folyamatairól és dologi viszonyairól szóló felvilágosítás.
Az érthető információk többnyire térben láthatóan - számok, betűk, szövegek és képek formájában, vagy időben hallhatóan - beszéd, zene és zajok formájában jelenhetnek meg.

Információ-feldolgozás: az informatikai rendszer által tárolt adatok különböző szempontok szerinti csoportosítása, különböző formában történő megjelenítése és továbbítása.

Információtárolás: az információ adattartalmának rögzítése, tárolása és módosítása.

Károkozás:

Szándékos károkozás:

- illetéktelen behatolás az informatikai rendszerekbe és azok környezetébe;
- informatikai adatok és eszközök eltulajdonítása vagy szándékos megrongálása;
- megtévesztő és hibás adatok rögzítése és képzése;
- adatkarbantartási és szoftverüzemeltetési műveletek szándékos elmulasztása;
- az információfeldolgozás zavarása és akadályozása;
- vírusos szoftver vagy adatállomány szándékos alkalmazása.

Nem szándékos károkozás:
- figyelmetlenség;
- hibás adatállomány kezelése;
- helytelen adatkezelés;
- szakmai hozzá nem értés;
- a szoftver- és hardverüzemeltetési előírások hiányos ismerete;
- adathordozók vétlen megrongálása (rossz tárolás-, szállítás, stb.);
- adatkarbantartási és szoftverüzemeltetési műveletek elmulasztása;
- vírusos szoftver vagy adatállomány vétlen/nem szándékos alkalmazása.

Kockázat: A kockázat matematikai fogalmakkal a rendszert ért váratlan eseményekből keletkező kár várható értéke adott időre vetítve. A kockázatokkal arányos a védelem, ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

Munkaállomás: egy operátor vagy felhasználó számára, adott típusú feladathoz felszerelt számítógép vagy terminál.

Rendelekzésre állás: Az informatikai rendszerelem -ideértve az adatot is- tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a szükséges időben és időtartamra használható.

Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, azaz egy információ vagy rendszer akkor sértetlen, ha csak az arra jogosultak változtathatják meg, vagy minden kétséget kizáróan megállapítható az a tény, hogy az előállítása óta változatlan maradt.

Szerver: olyan hálózatra kapcsolt központi szerepet betöltő számítógép, amelynek alapvető feladata, hogy más, a hálózatra kapcsolt számítógépek vagy terminálok számára az erőforrásait megossza.

Szerver terem: az a légkondicionált, biztonsági berendezésekkel ellátott helyiség, ahol a szerverek vannak, és csak a kijelölt köztisztviselők juthatnak be, regisztrálás után.

Szoftver: az informatikai eszközök fizikai lehetőségeit felhasználó eljárásokat leíró program. Szerzői jog hatálya alá tartozó szellemi termék.
Szoftverek általános csoportosítása:
- operációs szoftver-rendszerek – az informatikai eszközök használatát lehetővé tevő programok (pl. Windows 98, Windows XP);
- hálózati szoftver-rendszerek – az informatikai eszközök adatátviteli eszközökkel összekapcsolt hálózatának használatát lehetővé tevő programok (pl. Novell);
- általános célú felhasználói szoftverek – szövegszerkesztők, táblázatkezelők (pl. Word, Excel);
- egyedi felhasználói szoftverek - speciális feladatra készített számítógépes szoftverek (pl. ügyviteli programok, szakalkalmazások);

Vírus (számítógépes): olyan program, amely azzal a céllal készült, hogy informatikai rendszereket veszélyeztessen vagy tönkretegyen. Ezen vírusok léte az adatbiztonság legkritikusabb eleme, amely garantáltan kárt okoz és kizárólag megelőzéssel küszöbölhető ki.
A számítógépes vírus a felhasználói program vagy az adatállomány részeként terjed.

Vírusfertőzés (számítógépes):
Elszigetelt informatikai eszköz vagy hálózat nem képes vírust „előállítani".
Vírust kizárólag szoftver vagy adatállomány adathordozón történő átvételekor vagy adathordozó-hálózatról történő letöltésekor kaphatunk.
A „működő" vírus tevékenységei a fertőzés és a rombolás. A fertőzés a vírus terjedését jelenti, ahogy programfuttatás vagy adatátadás során önmagát sokszorozva "megfertőz" más, az informatikai rendszerben lévő szoftvert vagy adatállományt, a rombolás annak a „feladatnak" a végrehajtása, amiért a vírust létrehozták.

A vírusfertőzés általános tapasztalati jelei:
- az eddig „stabil" programok „lefagyása;
- a számítógép gyakori újraindulása vagy újraindítására irányuló jelzése;
- gyarapodó, indokolatlan számú adattároló (általában Winchester) használat;
- szokatlan vagy indokolatlan szövegek, adatok, jelek megjelenése;
- az alkalmazott szoftver eddig ismeretlen működése;
- a szoftverek alapállományainak, regisztrációs bejegyzéseinek indokolatlan sérülése, eltűnése.

3.5. Kötelezettségek a dokumentummal kapcsolatban

Felülvizsgálat, karbantartás:
A dokumentumot a számítástechnikában, informatikában, valamint a Hivatalban bekövetkező változások miatt időközönként aktualizálni kell. Évente felül kell vizsgálni, hogy a benne foglaltak időszerűek, érvényesek-e.
Ennek vizsgálata a Hivatal vezetője (jegyző) által kijelölt Informatikai felelős feladata.

Hatályba léptetés:
A szabályzatot a szervezet vezetője (jegyzője) a kihirdetését követő napon lépteti hatályba.

Kommunikáció:
A szabályzat változása esetén az annak hatálya alá tartozó személyeket és szervezeti egységeket –az elosztás rendje alapján- az új szabályzat jóváhagyását követő egy héten belül tájékoztatni kell.

IV.
A Szabályzathoz kapcsolódó jogszabályok

- 1978. évi IV. törvény - A Büntető Törvénykönyvről.
- 1992. évi LXIII. törvény - A személyes adatok védelméről, a közérdekű adatok nyilvánosságáról.
- 2001. évi CXXI. törvény - A Btk. módosításáról
- 2001. évi XXXV. törvény - Az elektronikus aláírásról
- 2001. évi CVIII. törvény - Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 1992. évi LXVI. törvény - A polgárok személyes adatainak nyilvántartásáról.
- 1987. évi 5. törvényerejű rendelet - Az állam és szolgálati titok védelméről.
- 16/1993.(XII.14.) BM rendelet a közszolgálati nyilvántartás egyes kérdéseiről.
- 1992. évi LXVI. tv. a polgárok személyi adatainak és lakcímének nyilvántartásáról.
- 1996. évi XXXI. tv. a tűz elleni védekezésről a műszaki mentésről és a tűzoltóságról.
- 4/1980.(XI.25.) BM rendelet az Országos Tűzvédelmi Szabályzat kiadásáról.
- 1995. évi LXV. tv. az államtitokról és a szolgálati titokról.
- 1969. évi III. törvény a szerzői jogról és a végrehajtására kiadott 9/1969.(XII.29.) MM rendelet.
- A Hivatal Adatvédelmi és Számítástechnikai védelmi szabályzata;
- A Hivatal Szervezeti és Működési Szabályzata;
- A Hivatal Munka- és Tűzvédelmi Szabályzata.

V.
Adatvagyonleltár

5.1. Szoftverek, szakalkalmazások

Szoftverek (op.rendszer, irodai alkalm.)	Mennyiség
Novell Netware 5.1	1
MS DOS 6.22	1
Microsoft Windows 98	9
Microsoft Windows XP	7
Microsoft Office	8
MagyarOffice	7

Szakalkalmazás neve	Funkció	Környezet / Mentés
Számadó	Főkönyvi könyvelés	Hálózatos / Központi
K11	Költségvetés és beszámoló készítő	Szólógép / Egyedi
Onkadó	Adónyilvántartó	Szólógép / Egyedi
IMI	Bér és munkaügyi prg.	Szólógép / Egyedi
ANAL	Analitika készítő	Szólógép / Egyedi
Mérleg	Mérleg készítő	Szólógép / Egyedi
Évközi	Évközi pénzügyi nyilv.	Szólógép / Egyedi
Házi pénztár	Házi pénztár	Szólógép / Egyedi
KataWin	Ingatlanvagyon kataszter	Hálózatos / Központi
OTP Ügyfélterminál	Banki utalások	Szólógép / Egyedi
Vizuál Regiszter	Népességnyilvántartás	Szólógép / Egyedi
WinSzoc	Szociális segélyezés	Szólógép / Egyedi
WinGyer	Gyámügyi nyilvántartás	Szólógép / Egyedi
Okmányirodai rendszerek, XR		Hálózatos / Központi
ASZA rendszer	Anyakönyvi rendszer	Hálózatos / Központi
Iktatás	Iktatás, iratkezelés	Szólógép / Egyedi
Tégla	Építéshatósági program	Szólógép / Egyedi

5.2. Hardverek, hálózat

Hardver eszközök	Mennyiség
File-szerver (Novell): Intel P4	1
PC számítógép konfigurációk (monitorral)	17
Tintasugaras nyomtatók	8
Lézernyomtatók	4
Mátrixnyomtatók	3
Belső hálózat UTP, 10/100Mbps	1
Switch (24TP)	1

VI.
Biztonsági osztályozás, kockázatelemzés

6.1. Az adatvagyon biztonsági besorolása

Az adatminősítés jelenlegi rendjét figyelembe véve az információ-védelem szempontjából a következő biztonsági osztályokat kell kialakítani:

- ***információ-védelmi alapbiztonsági (IV-A) osztály:***
  - Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.
- ***információvédelmi fokozott biztonsági (IV-F) osztály:***
  - A szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, banktitkok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya.
- ***információvédelmi kiemelt biztonsági (IV-K) osztály:***
  - Az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

Az önkormányzatok a IV-A osztályba tartoznak.

6.2. Informatikai kockázatelemzés

Jelen felsorolás a kockázatelemzés során feltárt, elviselhetetlen kockázatokat ismerteti, melyek csökkentésére védelmi intézkedéseket kell alkalmazni.

Fenyegető tényezők a környezeti infrastruktúra területén:

(F4) Villámcsapás
(F10) Gyújtogatás, sav, vandalizmus
(F11) Betörés
(F12) Áramellátás
(F13) Vízellátás
(F14) Jogosulatlan üzemen belüli személyek
(F15) Üzemen kívüli személyek
(F18) Takarítás
(F19) Elektromos szerelés
(F20) Telefonszerelés
(F21) Kábelfektetés
(F22) A kisegítő berendezések karbantartása
(F25) Informatikai komponensek karbantartása és üzembehelyezése

(F26) Ellátó és védelmi berendezések technikai hibája vagy kiesése
(F27) Tűzé (például rövidzárlat miatt)
(F28) Vízbetörés (például csőtörés miatt)

Fenyegető tényezők a hardver területén
(F33) A fő értékek vagy a levegő nedvességtartalmának felszökése vagy leesése
(F34) Piszkolódás (por, dörzspor)
(F37) A szoftver által kiváltott hibák a hardverben
(F41) Készülékek kikapcsolása,
(F43) Hamis adathordozók
(F47) Készülékek ellopása
(F48) Nyomtatóról (papír)
(F49) Képernyőről (különösen jelszavak)

Fenyegető tényezők az adathordozók területén
(F53) Lopás
(F56) Károsodás helytelen kezelés vagy tárolás miatt
(F57) Elöregedés miatti használhatatlanság (demagnetizálódás, mechanikai változások)
(F59) Már nem fellelhető adathordozók (nem szabályszerű tárolás)
(F61) Használhatatlanság a hiányzó kódoló, illetve dekódoló berendezések miatt
(F62) Használhatatlanság az inkompatibilis formátum miatt (logikai és fizikai értelemben)
(F65) Ismeretlen vagy kétséges eredetű adathordozók használata (szoftver-import)
(F66) Az adathordozók újrafelhasználásra vagy megsemmisítésre történő kiadása előzetes törlésük vagy átírásuk nélkül
(F70) Ellenőrizetlen másolás

Fenyegető tényezők a szoftver területén
Szoftverhiba
(F85) Hiba az alkalmazói szoftverben
(F86) Hiba az üzemelő rendszerszoftverben
(F87) Ismert hibák figyelmen kívül hagyása
(F88) A bejutás ellenőrzésének hiánya
(F90) A felhasználó figyelmetlensége
Nemkívánatos hozzáférés az alábbiak révén
(F91) Szükségtelen hozzáférési jogok (más felhasználók programjaihoz és adataihoz vagy rendszerprogramokhoz és rendszeradatokhoz)
(F93) Az üzemi rendszer ellenőrizetlen töltése
(F98) Kezelési hiba vagy visszaélés a kezelési funkciókkal

(F100) A szoftver sérülése, károsodása vagy használhatatlansága hardver hibák alapján

(F101) Jogosulatlan információnyerés a közösen használt üzemi eszközök révén

Fenyegető tényezők az alkalmazói adatok területén

(F102) Hardver hibák által keletkező adatvesztések, károsodások, eltérések

(F103) A szoftver által okozott adatvesztések, károsodások, eltérések (hibás vagy manipulált alkalmazói, illetve rendszerprogramok által)

(F104) Adathordozók által okozott adatvesztések, károsodások, eltérések

Emberek által okozott fenyegető tényezők

(F108) Jogosultak általi törlés/változtatás (tévedésből/szándékosan)

(F109) Jogosulatlanok általi törlés/változtatás (szükségtelen hozzáférési jogosultságok)

(F111) A bevitelek/kiadások elolvasása

Fenyegető tényezők a kommunikáció területén

A hálózatok elleni fenyegetések

(F116) A közvetítő-berendezések hibás viselkedése vagy kiesése műszaki hibák vagy hibás hálózati szoftverek miatt

(F117) Szabotázs/erőszakos cselekmény

(F118) Hálózati hardverek/szoftverek manipulálása

(F119) A fájlszerver kiesése vagy hibája helyi hálózatban

(F120) A többletérték szolgáltatások bizonytalan üzemeltetése a közüzemi hálózatokban

(F121) Zavaró befolyások (átviteli hibák)

(F122) Sérülés, károsodás

6.3. A védelem tárgya

- az alkalmazott hardver eszközök és azok működési biztonsága;
- a számítástechnikai eszközök üzemeltetéséhez szükséges okmányok és dokumentációk;
- az adatok és adathordozók megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig;
- az adatfeldolgozó programrendszerek, valamint a feldolgozást támogató rendszer-szoftverek tartalmi és logikai egysége, előírásszerű felhasználása, reprodukálhatósága;
- személyhez fűződő és vagyoni jogok;
- az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai;
- a munkakörnyezet fizikai biztonsága.

VII.
Szervezeti és személyi biztonság

7.1. Feladat- és jogkörök

A jegyző feladatai
A jegyző feladatát és hatáskörét az adatvédelem tekintetében a vonatkozó jogszabályok határozzák meg.
A Hivatal informatikai rendszerének kialakítása és üzemeltetése tekintetében a jegyző:

- jóváhagyja a szervezeti egységek vezetői által megállapított és az Informatikai felelős által kialakított (az egyes szervezeti egységeken belüli) jogosultsági rendszereket (szoftver, adattárak, Internet);
- jóváhagyja az Informatikai felelős által kialakított hivatali jelszórendszert;
- ellenőrzi a jogosultsági rendszert;
- kinevezi a Hivatal Adatvédelmi felelősét;
- informatikai adatvédelmi ellenőrzést kezdeményez, amely kiterjedhet az informatikai munkafolyamat bármely részére.
- ellenőrzi jelen Szabályzat betartását és betartatását;
- károkozás esetén kivizsgálást kezdeményez;
- jogosult a Hivatal informatikai rendszerei beállítási paramétereinek, az alkalmazott rendszerszoftverek és a mindenkori (alkalmazásban lévő) felhasználói szoftverek és adatállományok megismerésére és ellenőrzésére;

Informatikai felelős
A Hivatal informatikai rendszerének üzemeltetés-vezetője, a Hivatal informatikusa.

Az Informatikai felelős feladatai:

- ellátja és ellenőrzi az adatfeldolgozás felügyeletét és a védelmi előírások betartását;
- felelős az informatikai rendszerek üzembiztonságáért, a biztonsági másolatok készítéséért és karbantartásáért, az adatok archiválásáért;
- folyamatosan figyelemmel kíséri az informatikai rendszerek működését és a lényeges paraméterek alakulását;
- az informatikai eszközök külső szakemberrel történő javítása és karbantartása esetén a külső szakember tájékoztatása az adatvédelmi előírásokról;
- a szervezet informatikai infrastruktúrájának üzemeltetése és az ehhez kapcsolódó számítástechnikai, adatvédelmi szolgáltatások biztosítása;
- irányítja, segíti és ellenőrzi a munkatársak számítástechnikai munkáját;
- közreműködik a hardver és szoftver eszközök fejlesztésében, beszerzésében;
- elkészíti és évente ellenőrzi az Informatikai Biztonsági Szabályzat aktualitását

Az Informatikai felelős engedélyezési jogai:

- informatikai eszközök, szoftverek, adatállományok telepítése, áthelyezése, felújítása és selejtezése az Informatikai felelős engedélyével történhet;
- informatikai eszközök Hivatalból történő kiszállításához a Hivatal vezetője és az Informatikai felelős írásbeli engedélye szükséges.

Az Informatikai felelős helyettese adatvédelmi jogkörében a Hivatali Adatvédelmi felelős.

Hivatali Adatvédelmi Felelős

A Hivatali Adatvédelmi Felelőssel szemben támasztott követelmények:

- erkölcsi feddhetetlenség,
- vezetői összeférhetetlenség (összeférhetetlen minden olyan vezetői munkakörrel, ahol a napi munka szintjén adatvédelmi kérdésekben kell dönteni és intézkedni),
- felsőfokú szakirányú végzettség,
- informatikai alapszoftverek, hardver eszközök és védelmi rendszerek ismerete,
- informatikai rendszerek üzemeltetésének ismerete,
- az informatika szakterületére vonatkozó jogi szabályok és előírások ismerete.

A Hivatali Adatvédelmi Felelős a jegyző írásbeli meghatalmazása alapján jogosult ellátni feladatait.

A Hivatali Adatvédelmi Felelős általános feladatai:

- ellátja és ellenőrzi az adatfeldolgozás felügyeletét és a védelmi előírások betartását;
- felelős az informatikai rendszerek üzembiztonságáért, a biztonsági másolatok készítéséért és karbantartásáért;
- ellátja a számítástechnikai titokvédelmi munka szervezését és felügyeletét;
- a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében, a szakterületek bevonásával biztonságot növelő intézkedések kialakítása;
- folyamatosan figyelemmel kíséri az informatikai rendszerek működését és a lényeges paraméterek alakulását,
- adatvédelmi hiányosságok észlelése esetén haladéktalanul beszámol az Informatikai felelősnek és a jegyzőnek, valamint javaslatot tesz a hiányosság kiküszöbölésére;
- adatvédelmi feladatok ismertetése;
- a védelmi rendszer érvényesülésének felügyelete,

A Hivatali Adatvédelmi Felelős ellenőri feladatai:

- évente egy alkalommal részletesen ellenőrzi az Informatikai Biztonsági Szabályzat előírásainak betartását;
- évente adatvédelmi szempontból ellenőrzi az Informatikai Biztonsági Szabályzat aktualitását;
- a jegyző utasítására köteles informatikai adatvédelmi ellenőrzést folytatni, amely kiterjedhet az informatikai munkafolyamat bármely részére.

A Hivatali Adatvédelmi Felelős jogai:

- bármely hivatali szervezeti egységnél kezdeményezhet informatikai adatvédelmi ellenőrzést;
- az adatvédelmi előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a jegyzőnél;
- betekinthet valamennyi, az informatikai adatfeldolgozásokkal kapcsolatos iratba;
- adatvédelmi szempontból véleményezi az informatikai beruházásokat.

Az Adatvédelmi Felelős helyettese adatvédelmi jogkörében az Informatikai felelős.

Rendszerfelelős
A Polgármesteri Hivatal által alkalmazott egyedi felhasználói szoftverek üzemeltetésének megfelelő színvonalú támogatására és a helyi (irodai szintű) adatvédelem elősegítése céljából az alkalmazó szervezeti egységénél/egységeknél Rendszerfelelőst kell kinevezni.

A Rendszerfelelős feladatai:
- A Rendszerfelelős ellátja az alkalmazott egyedi felhasználói szoftver üzemeltetési feladatait.
- A Rendszerfelelős a felhasználói szoftver adatvédelmi felelőse.
- A Rendszerfelelős feladatait a Hivatal vezetőjének írásbeli meghatalmazása alapján látja el
- A Rendszerfelelős üzemeltetési feladatainak ellátása érdekében folyamatos szakmai kapcsolatot tart az Informatikai felelőssel, adatvédelmi feladatainak ellátása érdekében pedig a Hivatali Adatvédelmi felelőssel.

VIII.
Fizikai és környezeti biztonság

8.1. Az informatikai infrastruktúrát veszélyeztető helyzetek és a védekezés módszere

Közüzemi szolgáltatás zavarai (pl. 220 V-os tápfeszültség-kimaradás, feszültségingadozás, stb.). A feszültség-kimaradásra a számítógépes munkahelyekre telepített szünetmentes áramforrások szaggatott sípoló hangjelzéssel figyelmeztetnek. Ennek észlelése esetén azonnal meg kell kezdeni a folyamatban levő informatikai alkalmazási tevékenységek befejezését, majd az informatikai munkaeszközöket áramtalanítani kell.

A Hivatal épületébe történő illetéktelen behatolás észlelése esetén azonnal le kell zárni a helyszínt, értesíteni kell a Rendőrséget és a Hivatal vezetőjét. Haladéktalanul intézkedni kell a hiányleltár felvételéről.

Elemi csapás bekövetkezése esetén, annak fajtája (pl. villámcsapás, földrengés, stb.) szerint kell a szükséges intézkedéseket meghozni és a kárelhárítási tevékenységeket haladéktalanul meg kell kezdeni. A kárelhárítási tevékenységet szükség esetén külső szakszerviz bevonásával kell végezni.

A károsodás felmérése után azonnal meg kell kezdeni a rendszerek installálását. Amennyiben az eredeti helyszínen nem lehetséges a helyreállítás, más helyen szükséges a rendszerek beüzemelése.

Környezeti kár (pl. légszennyezettség, nagy elektromágneses térerő, fokozott tűz- és robbanásveszély, stb.) esetén fel kell mérni a kár mértékét és fajtáját, és külső szakszerviz bevonásával kell végrehajtani a mentést. A károsodás észlelése és felmérése után azonnal meg kell kezdeni a rendszerek installálását. Amennyiben az eredeti helyszínen nem lehetséges a helyreállítás, más helyen szükséges a rendszerek beüzemelése.

Az informatikai rendszerek részleges vagy teljes károsodása esetére „Katasztrófa Terv"-et kell készíteni, amely a következőket tartalmazza:

- a még használható eszközök felmérési és mentési módszerének leírása;
- az ideiglenes adatfeldolgozási hely kijelölésének szempontjai;
- az ideiglenes hely kialakításának módja;
- a megsérült adatok, szoftverek helyreállításának módszerei;
- ideiglenes szoftver- és hardverbázis biztosításának lehetőségei;
- az eredeti állapot visszaállításának folyamata.

A „Katasztrófa Terv"-et a Jegyző hitelesíti és hagyja jóvá.

Szándékos károkozás észlelése vagy gyanúja esetén a Hivatal dolgozója köteles jelenteni azt közvetlen felettesének vagy a Jegyzőnek.

A **nem szándékos károkozásból** eredő kár elhárítását az észlelést követően azonnal meg kell kezdeni és az ismétlődő előfordulást ki kell küszöbölni.

8.2. Informatikai védelmi eszközök

Általános védelmi eszközök
Az általános védelmi eszközök azok a jogi, műszaki, szervezési és programozási előírások, szabályok és intézkedések, amelyek az adatok általános védelmét biztosítják.

Fizikai védelmi eszközök, vagyonvédelem
A fizikai védelem a biztonságos munkakörnyezet megteremtését jelenti.
A fizikai védelem részei:

- Az ügyfélszolgálati idő pontos betartása;
- Az ügyfélszolgálati idő alatt az ügyfélszolgálattal nem foglalkozó irodák elhagyása esetén az ajtók zárása, az adattároló szekrények zárása;
- Az informatikai adatfeldolgozó munkahelyekhez való illetéktelen hozzáférés lehetőségének kizárása;
- Az adatfeldolgozó számítógép monitorának oly módon történő elhelyezése (elfordítása vagy eltakarása), hogy az azon megjelenő adatokat illetéktelen személyek ne láthassák, illetve ne értelmezhessék (üres képernyő politika);
- A számítógépes és a hagyományos feldolgozású adatok, adathordozók megfelelő tárolásának és elzárásának biztosítása;
- Az informatikai rendszerszoftverek, egyedi felhasználói szoftverek, rendszerleírások, rendszerdokumentációk, jogosultsági adatok, indítólemezek, védelmi jelszórendszerek, archivált adatállományok, mentések kettő példányban történő biztonságos (tűz- és lopás elleni) tárolása;
- Az irodaajtók kulcsainak biztonságos tárolása, az informatikai rendszerek kiemelt védelmet igénylő eszközeit tároló irodák ajtajára biztonsági zárak felszerelése;
- A meglévő biztonságtechnikai rendszer (behatolásvédelem, riasztó és tűzjelzés) megfelelő és folyamatos működtetése és jogosultság szerinti használata;
- A tűzvédelmi előírások betartása a Hivatal „Tűzvédelmi Utasítása" alapján;
- Elemi csapások és egyéb káros környezeti hatások lehetőség szerinti kivédése, az okozott kár mérséklésére való törekvés;
- Az informatikai eszközök rendeltetésszerű működtetése és használata.

Adminisztratív védelmi eszközök
Az adminisztratív védelmet a munkavégzésre vonatkozó és annak módját meghatározó előírások és szabályok összessége jelenti, amelynek részei:

- A rugalmas munkaidő alkalmazásáról szóló szabályzat előírásainak betartása;
- Az ügyirat kezelési szabályzat előírásainak betartása;
- Az iratmásolás és sokszorosítás rendjének betartása;
- A bélyegzők kezelésére és használatára vonatkozó előírások betartása;

Speciális védelmi eszközök
A speciális védelmi eszközök az informatikai környezet (hardver, szoftver) védelmét szolgáló eszközök és módszerek összessége, amelyek a vészhelyzetek megelőzésére és észlelésére, valamint a bekövetkezett károk mérséklésére és az eredeti állapot mielőbbi helyreállítására irányulnak.

A speciális informatikai védelmi eszközök elemei:

- Az adatbiztonságot támogató hardvertípus, operációs rendszer, hálózati és egyedi felhasználói szoftver alkalmazása;
- A hálózati név- és jelszórendszer bizalmas alkalmazása és évenkénti változtatása (kiépített hálózat esetén);
- Az egyéni jelszavas hálózati jogosultsági rendszerrel a felhasználói szoftverek és az adatállományok hozzáférési jogosultságának szabályozása;
- A vírusvédelem szabályainak betartása;
- A kémprogramok elleni védelem szabályainak betartása;
- Az internet használat szabályainak betartása;
- Az internetről történő letöltések szabályainak betartása;
- Az elektronikus levelezés szabályainak betartása;
- Az adatállományok rendszeres mentése és archiválása;
- Különleges, egyedi feladatok végzése alkalmával, szükség esetén speciális biztonsági intézkedések megtétele (pl. választások előkészítése és kiértékelő feldolgozása);

8.3. Az informatikai védelem specifikus szabályai

Üzemeltetési Napló

A Hivatal azon számítógépes munkahelyein, ahol azt az Informatikai felelős és a hivatal vezetője indokoltnak tartja „Üzemeltetési Napló"-t kell vezetni.
Az Üzemeltetési Napló vezetésének célja a rendeltetésszerű működéstől való eltérés és az indokolt beavatkozások (hardver-szoftver-adatállomány tekintetében) rögzítése.
Adattartalmát az Informatikai felelős határozza meg.
Az Üzemeltetési Napló kiadása az Informatikai felelős, hitelesítése a Hivatal vezetőjének feladata.

Az Üzemeltetési Napló vezetése a Rendszerfelelősnek, az adott felhasználói szoftver alkalmazójának és az Informatikai felelősnek a feladata. Mindennemű külső beavatkozást az Üzemeltetési Naplóban rögzíteni kell.
Az Üzemeltetési Napló vezetését az Informatikai felelős és az Adatvédelmi felelős negyedévenként ellenőrzi. Az ellenőrzés tényét és a feltárt hiányosságokat az Üzemeltetési Naplóban rögzítik. A feltárt hiányosságokról a jegyző részére feljegyzést készítenek.

A vírusvédelem szabályai

A Hivatalban alkalmazott informatikai rendszer minden adatbeviteli elemén kiemelten kell kezelni a vírusvédelmet, mivel a vírusfertőzés veszélye folyamatosan fennáll.
Vírus külső adathordozón, illetve az interneten keresztül kerülhet a Hivatal informatikai rendszerébe, ezért a fentiek vírusellenőrzése minden esetben kötelező.

A vírusvédelemmel kapcsolatos szabályok:

- idegen adathordozót, szoftvert és adatállományt a Hivatalban alkalmazásba állítani csak az Informatikai felelős által elvégzett vírusellenőrzés után lehet. Minden egyéb használatból történő kár és hátrány az adathordozót használatba vevő felhasználót terheli;

- a számítógépek beüzemelését és a vírusvédelmi megoldás telepítését, paraméterezését csak az Informatikai felelős végezheti;
- a munkaállomásokon és szervereken, ha másképp nincs rendelkezés, heti rendszerességgel vírusellenőrzést és vírusirtást kell tartani;
- vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az Informatikai felelősnek;
- amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni;
- a gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes szakember (Informatikai felelős), meg nem vizsgálta;
- a vírusfertőzést jelenteni kell a Hivatal vezetőjének és az Informatikai felelősnek, még akkor is, ha semmi hiba nem történt a fertőzés folyamán;
- az Informatikai felelősnek ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia;
- a vírusvédelmi rendszert rezidens módon kell beállítani, azaz úgy, hogy a rendszerindításkor elinduljon és folyamatosan fusson;
- a vírusfertőzés tényét naplózni kell, az így keletkező riportot (naplóállományt) ki kell nyomtatni és le kell fűzni az Üzemeltetési Naplóba

Az internetről történő letöltések szabályai

- ha a felhasználó bizonytalan egy melléklet felől, inkább törölni kell, főleg akkor, ha az egy azonosítatlan helyről származik;
- óvakodni kell az olyan fájlok letöltésétől, amelyekről nem tudható kétséget kizáróan, hogy biztonságosak;
- a letöltésekhez célkönyvtárként egy központi helyet kell kinevezni a helyi gép merevlemezén a könnyebb visszakereshetőség és ellenőrízhetőség végett

Az elektronikus levelezés szabályai

- a levelezőprogramot úgy kell paraméterezni, hogy a letöltött leveleket fizikailag legalább 5 napig a kiszolgálón meghagyja;
- vírusvédelmi rendszernek a beérkező e-mail-t minden esetben vizsgálnia kell az összes csatolmányával együtt;
- be kell állítani, hogy a levelezőprogram ne nyissa meg automatikusan a mellékleteket;
- a levélhez tilos csatolni exe, com és bat kiterjesztésű file-okat. Ha ilyen kiterjesztésű állományok érkeznek e-mail-ben, akkor azok futtatása előtt az informatikussal egyeztetni kell. A feladót meg kell kérni, hogy ha teheti, ne küldjön a fent felsorolt file-kiterjesztésekkel csatolt állományt. Ha a feladó és a levél célja, tartalma ismeretlen akkor, az e-mailt törölni kell.
- Rendszeres vagy tervezett adatcsere során törekedni kell a doc és xls kiterjesztésű file-ok használatának mellőzésére is. Helyette rtf vagy pdf, és dbf vagy txt az ajánlott.
- A vírusok jelentős része képes beépülni az előző pontban felsorolt típusú file-okba. Az ismert és ismeretlen vírusok terjedése ezzel a kikötéssel megakadályozható.

Az adatállományok rendszeres mentése és archiválása

- a rendszeres mentések végzése az adott szakalkalmazást üzemeltető ügyintéző feladata (a felhasználói szoftverleírások és az Informatikai felelős

által kidolgozott „Mentési Rend"-nek megfelelően), az Informatikai felelős szakmai felügyeletével.
- az évenkénti és az egyedi (pl. választási adatok) archiválások és mentések végzése az Informatikai felelős feladata, a lefektetett „Mentési Rend" szerint.

Az alkalmazott szoftverekkel és adatállományokkal kapcsolatos védelmi előírások
- Az adatállományok védelmi szabályainak betartása az adatállományért felelős dolgozó feladata.
- Az adatvédelem tekintetében folyamatosan alkalmazni kell a törvényi és egyéb jogszabályi előírásokat az adatok felvételére, tárolására, átadására, kezelésére és archiválására vonatkozóan.

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

közlésre szánt (bárki által megismerhető) adatok,
minősített adatok (titoknak minősülnek).

- A számítógépes feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme hatáskörébe tartozik.
- A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névreszólóan a hozzáférési jogosultságot.
- A kijelölt köztisztviselők előtt a titokvédelmi és egyéb rendszabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.
- A titkot képező adatok védelmét, a feldolgozás - adattovábbítás, tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott titkosítással, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftveres és hardveres adatvédelem).
- A szoftverek, adatállományok és informatikai eszközök üzembe állítását kizárólag az Informatikai felelős végezheti.
- Szoftvermásolatok készítésére ill. archivált adatállományokból történő másolatok és leválogatások készítésére az Adatvédelmi felelős illetve az Informatikai felelős jogosult, a vonatkozó adatvédelmi és szerzői jogi védelmi előírások betartásával.
- Az informatikai alapú adatállományok megőrzésére, selejtezésére és megsemmisítésére a Hivatal Iratkezelési Szabályzatának előírásait kell alkalmazni.

Egyéb adatvédelmi előírások:
- az adatbevitel hibátlan műszaki állapotú berendezésen történjen;
- csak tesztelt adathordozóra lehet adatállományt rögzíteni;
- a programokat és az adatokat ellenőrző funkciókkal, amennyiben szükséges titkosítással kell ellátni;
- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen hozzáférési szinten férhet hozzá a programokhoz és adatokhoz (a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá);
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

A szoftvervédelem egyéb szabályai

- az Informatikai felelősnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az illetékes felhasználók számára.

Rendszerszoftver védelem:

- a rendszerszoftver módosításához az illetékes engedélye szükséges,
- a módosítással egy időben a dokumentációban is át kell a változtatásokat vezetni,
- a rendszerszoftver-eseményekről és a változtatásokról nyilvántartást kell vezetni (eseménynapló).

Programhoz való hozzáférés, programvédelem:

- a kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni;
- gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek;
- a feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a programok dokumentációit

A programokról nyilvántartást (Szoftver leltárt) kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a program azonosítója,
- a program készítőjének neve,
- a feldolgozási rendszer megnevezése.

Programok fizikai védelme:

- A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten, egy-egy duplikált példányt kell tárolni

Hardver védelem

- A számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől;
- a számítógép közelében ételt és italt fogyasztani tilos;
- a számítógépteremben és a szerver teremben (kiépített hálózat esetén) klímaberendezés használata ajánlott;
- szervereknél és munkaállomás gépeknél a szünetmenetes áramforrással való ellátást biztosítani kell;
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez,
- havi rendszerességgel a számítógépeken hardver teszteket kell lefuttatni.

Adatszolgáltatás

- Külső szervezet részére adatszolgáltatás történhet adathordozón, nyomtatott formában és Interneten keresztül;
- A Hivatal szervezeti egységei és az Adatvédelmi felelős külső személy/szervezet részére történő adatszolgáltatást kizárólag jogszabályi előírás vagy Jegyzői utasítás alapján végezhetnek.
- Hivatalon belüli -jogszabályban nem rögzített- informatikai alapú adatszolgáltatást az Adatvédelmi felelős kizárólag a Hivatal vezetője engedélyével végezhet.

IX.
Védelmi intézkedések

A kockázatok mérséklésére alkalmazható védelmi intézkedések az itt található felsorolásából kiválaszthatóak. Eldöntendő hogy melyek a már bevezetett, létező és működő intézkedések, illetve melyek azon intézkedések, melyeket szükséges mindenképp bevezetni a fennálló kockázatok csökkentésére.

9.1. Általános jellegű biztonsági intézkedések

Belépés, benntartózkodás:

(I1) Az üzem területére való belépés (személyek és járművek) ellenőrzése, például bekerítés és őrzött bejáratok révén.
(I2) Az épületekbe és a helyiségekbe való belépés ellenőrzése, például portások vagy technikai berendezések révén (kulcsok, igazolványolvasók stb.)
(I3) A belépés jegyzőkönyvezése, például számítógép-vezérelt ellenőrző rendszerekkel.
(I4) Az üzemen kívüli személyek tartózkodásának figyelemmel kísérése (állandó kíséret vagy regisztrálás révén).
(I5) A bejutást biztosító fizikai azonosítási eszközök (például kulcsok és chipkártyák) kiadása, regisztrálása és visszavétele.
(I6) A bejutást biztosító jelszavak kiválasztásának és kezelésének szabályozása (ne lehessen a saját név variációja, a szótárból vett szó, személyes adat stb.).
(I7) Központi felhasználó-adminisztráció (például a felhasználó felismerésének hiánya jelszó nélkül, kikényszerített jelszó-váltás, a kieső munkatársak jelzéseinek törlése vagy zárolása stb.).
(I8) A kritikus (nem ellenőrizhető) cselekvési területek azonosítása (például laptopok, túlórák, otthoni munka, rendszerkezelés / igazgatás).
(I9) A kriptográfiai kulcsok kezelése és elosztása.
(I10) Szoftvermechanizmusok bevezetése a bejutást biztosító jelszavak kezelésének, minőségének, érvényességének ellenőrzésére.
(I11) Hitelesítési eljárások alkalmazása (például chipkártyák, biometrikus eljárások).
(I12) Bejelentkezés lehetőségének zárolása hibás kísérletek után.

Jogosultságok és szerepek:

(I13) A védelemigényes helyiségekbe vagy zónákba való belépési jogosultságok szabályozása.
(I14) A személyek és személyek csoportjai hozzárendelése a helyiségekhez az informatikai rendszerben vagy környezetében betöltött szerepük alapján.
(I15) A belépésre jogosító segédeszközök kiadása és visszavétele (például kulcsok, igazolványok, kódszámok).
(I16) Az adatokhoz, alkalmazói programokhoz, rendszerprogramokhoz való hozzáférés jogának (olvasás, írás, kifejtés) hozzárendelése azokhoz a személyekhez és a személycsoportokhoz, akiket szerepük erre predesztinál.
(I17) A hálózatba való bejutási jogok odaítélése, felépítése, figyelemmel kísérése és jegyzőkönyvezése (szervezési, informatikai intézkedések).
(I18) A jogok továbbadásának szabályozása és korlátozása.

(I19) A jogosultsági struktúra periodikus, szúrópróbaszerű, vagy alkalomhoz kötődő átvizsgálása (például megváltozott feladatmegosztás esetén).
(I20) A végrehajtó/megvalósító és ellenőrző funkciók személyi szétválasztása.
(I21) Az ellenőrző funkciók explicit definiálása (hatókör, eszköz, alkalom stb.).
(I22) A végrehajtási/megvalósítási funkciók strukturálása:
- funkcionális szétválasztás (a részfeladatokat különböző személyek végezzék) a rendszerkezelésnél, az adatfeldolgozás ellenőrzésénél
- négy szem elv (a kritikus feladatokat két személy oldja meg)
- minimális jogok odaítélése

(I23) A védelmi eszközökhöz kapcsolódó menedzsment feladatok meghatározása, végrehajtása és ellenőrzése, pl. intézkedések a rejtjelezés kulcsainak igazgatására, kezelésére, adminisztrációjára (előállítás, átadás, csere, titoktartás).

Ügyintézés, adminisztráció:

(I30) A rendszer eseményeinek jegyzőkönyvezése (például hardverhibák vagy automatikus újraindítás bekövetkezte).
(I31) A felhasználói tevékenységek jegyzőkönyvezése (például felhasználási idő, eszközök használata, fájlokhoz való hozzáférés, adatátvitel).
(I32) A biztonsági szempontból releváns különleges események jegyzőkönyvezése (például hamis jelszóval való bejutási kísérletek, jogosulatlan hozzáférési kísérletek).
(I33) A biztonsági szempontból releváns programtevékenység figyelemmel kísérése, jelentése vagy félbeszakítása (jegyzőkönyvezés).
(I34) A jegyzőkönyvi adatok program által támogatott elemzése.
(I35) A jegyzőkönyvi adatok archiválása (manuálisan, gépileg).
(I36) A jegyzőkönyvi adatok védelme illetéktelen hozzájutástól, utólagos módosítástól.
(I37) A maradványkockázatok lefedése biztosítási szerződésekkel (anyagi ellentételezésre vonatkozó szerződések biztosító intézkedésekkel).
(I38) A biztonsági intézkedések betartásának ellenőrzési rendszere, kötelező reakciók előírása a szabályok megsértése esetén.

A fent felsorolt intézkedések a következő fenyegető tényezők hatását mérséklik:

- (F1)-(F11), (F14)-(F25), (F27), (F28) - a környezeti infrastruktúra területén,
- (F46), (F47) - a hardver területén,
- (F53), (F67)-(F70) - az adathordozók területén,
- (F80)-(F82), (F84) - a dokumentumok területén,
- (F88), (F89), (F91), (F92), (F101) - a szoftver területén,
- (F109), (F112) - az adatok területén,
- (F148) - a személyek csoportjában.

9.2. Biztonsági intézkedések a környezeti infrastruktúra védelmében

Tűzvédelem

(I39) A tüzek keletkezésének megakadályozása (például a dohányzás tilalmával, a szabványnak megfelelő elektromos szereléssel).
(I40) A tüzek kiterjedésének gátlása (például tűzbiztos válaszfalakkal, ajtókkal, nehezen éghető belső borításokkal).
(I41) Tűzjelzés (például automatikus szenzorokkal vagy kézi tűzjelzővel).
(I42) Tűzoltás (például automatikus elárasztókkal, kézioltókkal).
(I43) A számítógéptermek illetve helyiségek tűzvédelmi kialakítása.

Villámvédelem

(I44) Az épületé villámhárítóval.
(I45) Az informatikai készülékeké az indukált túlfeszültségekkel szemben (például a készülékek leválasztása az elektromos hálózatról, az adathálózat szakaszolása galvanikusan elkülönített részhálózatokká).

Vízvédelem

(I46) Passzív intézkedésekkel (például a helyiségek kijelölése a pinceszint fölött).
(I47) Aktív intézkedésekkel (például vízlevezetők, szivattyúk).

Az áramellátás védelme

(I48) Rövid ideig tartó feszültségcsökkenések kiküszöbölése (például szünetmentes áramellátást biztosító készülékek, akkumulátorok alkalmazásával vagy redundanciával a készülékeknél és vezetékeknél).
(I49) Feszültségkiesés áthidalása (például szükségáramot biztosító aggregátorral).

A klímaellátás biztosítása

(I50) Automatikus szabályozó berendezésekkel optikai vagy akusztikus kijelzéssel a toleranciaszintek túllépése esetén.
(I51) A szellőzőnyílások karbantartásával.

Védelem a befolyásolhatatlan külső tényezők ellen

(I52) Telephelytervezés (például ne a berepülési útvonalba stb.).
(I53) Erősítő intézkedések (például az épület konstrukciójánál).

Védelem külső támadások ellen

(I54) Telephely-/helyiségtervezés (például a számítógép központnak ne legyen a nyílt utcán, a földszintje, ne legyen kívülről belátható).
(I55) Az elhelyezésre utaló nyílt útmutatások elkerülése (például, ne legyen útjelző a számítóközponthoz, és jelzőtáblák az épületek és a helyiségek bejáratánál).

Betörésvédelem

(I56) Megelőző intézkedések (például rácsos ablakok, az áttörést nehezítő üvegezés, acélajtók, speciális zárak).
(I57) Behatolás-érzékelők felszerelése.

Sugárzásvédelem

(I58) A teremsugárzás megakadályozása teljes leárnyékolással (például Faraday kalitkával elvben egyenértékű kialakítású helyiség kialakításával, a vezetékek vascsövekben történő elhelyezésével, optikai kábelek alkalmazásával).
(I59) A teremsugárzás kivédése részleges leárnyékolással (például kabinok vagy házak, tárolók az egyes készülékek számára, kisugárzásvédett képernyők alkalmazása, elhelyezés ellenőrzött biztonsági zónákban).
(I60) Fémvezetékek rácsatlakozás elleni védelme (szűrő az áramvezetékekben, szűrő az átviteli vezetékekben, galvanikus megszakítás a fűtő- és vízvezeték-csövekben stb.)
(I61) Védekezések a zavaró besugárzások ellen (Faraday kalitkával, galvanikus leválasztásokkal, optikai kábel összeköttetésekkel

Ebben a csoportban felsorolt intézkedések a következő fenyegető tényezők hatását mérséklik:

- (F1)-(F4), (F6), (F11), (F12), (F27), (F28) - a környezeti infrastruktúra területén,
- (F32), (F33), (F35), (F51) - a hardver területén,
- (F53), (F55), (F58) - az adathordozók területén,
- (F123), (F127) - a kommunikáció területén.

9.3. Biztonsági intézkedések a hardver védelmében

(I62) Megállapodás a hardver-szállítókkal a garantált javítási, illetve cserélési feltételekről és határidőkről.
(I63) Az informatikai készülékek koncentrált elhelyezése révén a belépés ellenőrzésének megkönnyítése
(I64) Csak centralizált beviteli/kiviteli eszközök alkalmazása a külső adathordozók számára.
(I65) Rendszeres megelőző karbantartás.
(I66) A különösen érzékeny komponensek megelőző cseréje.
(I67) Elzárkózás a legújabb, még nem kipróbált termékektől.
(I68) Redundáns, hibatűrő konfigurációk.
(I69) Pótalkatrészek készletezése.
(I70) Az ergonómiai szempontok figyelembevétele a hardverválasztásnál és -kiépítésnél (pl. a képernyő villódzása, zaj, stb.).
(I71) Manipulációbiztos készülékek beszerzése (pl. olyanoké, amelyek zárható házban kerülnek forgalomba).
(I72) A készülékek rendszeres felügyelete biztonsági szempontokból.
(I73) A hardver környezeti feltételeinek ellenőrzése.
(I74) A számítógépekbe és a hálózatba való bejutás módozatainak szabályozása.
(I75) A hardver eszközök, illetve szolgáltatásaik igénybevétele csak a felhasználó azonosítását és hitelesítését követően legyen lehetséges.
(I76) Hosszabb inaktivitás esetén kényszerített kijelentkezés vagy a berendezés "blokkolása" (például képernyőzárolás).
(I77) A fejlesztő és a végrehajtó számítógépek szigorú elhatárolása (felhasználói gépen nem folyhat szoftverfejlesztés).

(I78) Katasztrófa-megelőzés, illetve "túlélés" érdekében alternatív cselekvési forgatókönyvek összeállítása a különböző típusú, kiterjedésű és tartalmú kiesésekre nézve (például egyes készülékek vagy a számítóközpont teljes szétrombolása, roncsolódása).
(I79) Az alkalmazott rendszer valamennyi készülékéről, azok műszaki állapotváltozásairól és konfigurálásáról folyamatos nyilvántartás (műszaki törzslap) vezetése.

Ebben a csoportban felsorolt intézkedések a következő fenyegető tényezők hatását mérséklik:

- (F1)-(F13), (F26)-(F28) - a környezeti infrastruktúra területén,
- (F28)-(F36), (F44)-(F47), (F50) - a hardver területén,
- (F54)-(F58) - az adathordozók területén,
- (F88), (F89), (F95) (F98) - a szoftver területén,
- (F102), (F109) - az adatok területén,
- (F114), (F115) (F119) (F122) - a kommunikáció területén.

9.4. Biztonsági intézkedések az adathordozók védelmében

(I80) Adathordozó-adminisztráció kialakítása (beszerzés, gazdálkodás, készlet- és használat nyilvántartás, selejtezési eljárás, az utánpótlás megszervezése stb.)
(I81) Külön, belépés-ellenőrzéssel ellátott adathordozó tároló helyiség kialakítása.
(I82) A környezeti körülmények ellenőrzése (hőmérséklet, nedvességtartalom stb.).
(I83) Megelőző intézkedés az elöregedés és a már nem preferált formátumok vonatkozásában (átmásolás).
(I84) Törlés a felszabadítás, kiselejtezés előtt.
(I85) Katasztrófa-megelőzés céljából a másodpéldányok kiemelten biztonságos (más telephelyen történő) raktározása.
(I86) A beszerzett adathordozók ellenőrzése az alkalmazásra való felszabadításuk előtt.
(I87) Előírások az adathordozók felhasználói számára (védelem rongálódás ellen, külső jelölés, védelem jogosulatlan használattól stb.).
(I88) Az előállított adathordozók ellenőrzése (újraolvashatóság).
(I89) Az adathordozók tartalmának védelme (kódolás, rejtjelezés, olyan jelölés, amely nem tartalmaz közvetlen utalást a tartalomra, kódoló, dekódoló eszközök használata stb.).
(I90) Privát adathordozók szolgálati célokra vagy fordítva történő igénybevételének tilalma.
(I91) A kölcsönzés, a regisztrálás, a visszaadás eljárása.
(I92) Az adathordozók ellenőrzött kiselejtezése.

Ebben a csoportban felsorolt intézkedések a következő fenyegető tényezők hatását mérséklik:

- (F1)-(F13), (F26)-(F28) - a környezeti infrastruktúra területén,
- (F28)-(F36), (F44)-(F47), (F50) - a hardver területén,
- (F54)-(F58) - az adathordozók területén,
- (F88), (F89), (F95) (F98) - a szoftver területén,
- (F102), (F109) - az adatok területén.

9.5. Biztonsági intézkedések a dokumentumok védelmében

(I93) A hardver és szoftver dokumentációk, kezelői utasítások beszerzésének, aktualizálásának, tárolásának, rendelkezésre állásának szabályozása.
(I94) A szükséges dokumentációk, szoftverek és hardverek nyilvántartása valamennyi informatikai alkalmazás esetére (programok, adatállományok, pótlólagos szoftverek, beviteli és kiadási készülékek, tároló- és időigény stb.).
(I95) Biztonságspecifikus előírások az üzemviteli jegyzőkönyvek kiértékelésére és archiválására.
(I96) Eljárás szabályozása az informatikai dokumentumok másolása, kölcsönzése esetére.
(I97) A dokumentumok sértetlenségének biztosítása.
(I98) A dokumentum selejtezési eljárása.

Ebben a csoportban felsorolt intézkedések a következő fenyegető tényezők hatását mérséklik:

- (F53), (F71)-(F84) - a dokumentumok területén,
- (F96), (F98) - a szoftver területén,

9.6. Biztonsági intézkedések a szoftver védelmében

(I99) Elfogadható biztonsági osztályú rendszer kiválasztása, pl egy minősítő hatóság (esetleg a szállítótól bekért) minőségtanúsítványa alapján.
(I100) Új, instabil szoftver verziók bevezetésének késleltetése a megfelelő minőségellenőrzési eredmények megszületéséig.
(I101) Ismert hibájú szoftver használatának elkerülése, illetve -szükséghelyzetben- gondosan ellenőrzött használata.
(I102) Az üzemi eszközhasználat vizsgálata az abnormitások vonatkozásában.
(I103) A teljes szoftver sértetlenségének rendszeres ellenőrzése.
(I104) Szoftver minőségellenőrzés különálló számítógépen lefuttatott teszt segítségével.
(I105) A hardver és a szoftver funkcionális tesztprogramjainak rendszeres használata (például a fájlrendszer konzisztenciájának rendszeres ellenőrzése).
(I106) Felhasználóbarát kezelői felületek bevezetése (pl. menüvezérlés, ablaktechnika).
(I107) A rendszer- és alkalmazói programok sértetlenségének védelme helyi hálózatokban központi szerverről történő programindítás segítségével.
(I108) Vírus ellenőrzött programok használata.
(I109) Idegen szoftverek ellenőrizetlen bevitelének tilalma.
(I110) Privát szoftverek szolgálati célokra, illetve a szolgálatiak privát célokra való alkalmazásának tilalma.
(I111) A szoftver felszabadítása és elosztása kizárólag az erre a tevékenységre feljogosított személyek által az alkalmazás kontrollja és az eltulajdonítás megelőzése érdekében.
(I112) A bevezetett alkalmazás-független szoftverek és bizalmassági feltételeik (például verziók közötti kompatibilitás) kimutatása

- üzemi rendszerekre és rendszerközeli bővítésekre (például Windows rendszerek),

- pótlólagos szoftverekre (például adatbázisrendszerek, editorok, grafikus szoftverek),
- biztonsági célokra elkülönített szoftvercsomagok (például illegális bejutás ellenőrzése, vírusfelismerés).

(I113) A rendelkezésre álló funkcionalitás behatárolása bizonyos felhasználók és hosszabb inaktivitás esetén felhasználócsoportok számára (például szövegszerkesztők vagy fordítóprogramok használatának tiltása, a rendszerprogram-szint zárolása, a rendelkezésre álló parancsok körének szűkítése).
(I114) Többszintű hozzáférési rendszer használata (például külön jogosultság az adatbázis-rendszerben, levelező rendszerben stb.).
(I115) Rendszer-adatállományok és parancsok használatának korlátozása (pl. a rendszerkezelőre).
(I116) A biztonsági vonatkozású adatállományok, rendszerprogramok helyességének és konzisztenciájának fenntartása, pl. program által támogatott konzisztenciavizsgálat
(I117) Utasítások kiadása

- a biztonsági futtatások elvégzésére, jegyzőkönyvezésére és átvizsgálására,
- az újrafuttatási és rekonstrukciós eljárásokra,
- a szoftver sértetlenségének igazolására (pl. ellenőrző összegek segítségével),
- a szoftvert tartalmazó adathordozók jelölésére és gondozására.

(I118) Az informatikai rendszer, a Kontroller Iktató, Ügyiratkezelő rendszer üzemeltetési előírásai.
(I119) Intézkedések a karbantartási munkálatok előtti és utáni tevékenységekre (pl. az üzemi rendszer betöltése külső adathordozóról) a szoftver sértetlenségének és bizalmasságának biztosítása érdekében.
(I120) A felhasználói szoftverfejlesztés megakadályozása.
(I121) A felhasználói és rendszerszoftverek törzspéldányainak biztonságát szolgáló tárolási, kezelési előírások.

Ebben a csoportban felsorolt intézkedések a következő fenyegető tényezők hatását mérséklik:

- (F30)-(F43) - a hardver területén,
- (F65) - az adathordozók területén,
- (F53), (F85)-(F101) - a szoftver területén,
- (F103), (F106) (F107) - az adatok területén.

9.7. Biztonsági intézkedések az adatok védelmében

(122) Üzemviteli előírások

- adatbiztosításra (mentés, helyreállítás, őrzési időtartam stb.),
- elkülönített területek a látogatók forgalmára (adatbeviteli, kiadási műveletek elszigetelése),
- adatterületek törlése az operatív tárban újra felhasználás előtt,
- adatállományok tárolása kódolással, ellenőrzőösszeg alkalmazásával, digitális aláírással, redundáns tárolással (pl. lemeztükrözés) stb.

(I123) Intézkedések karbantartási munkálatok előtt és után a szoftver és az adatok sértetlenségének és bizalmasságának biztosítása érdekében (például a bizalmas adatállományok biztosítása és törlése).
(I124) Tranzakció-kezelés alkalmazása, pl. adatbázis-rendszereknél.

(I125) Adatvesztés elleni biztosítás osztott rendszerekben bekövetkezhető centralizált adattárolással, például fájl szerver helyi hálózatokban.
(I126) Védelem hibás adatbevitel és adatváltoztatás ellen az alkalmazói programokban szereplő formátum, valamint konzisztencia ellenőrzésekkel.
(I127) Manuális pótlások, esetleges szükségeljárások előírásai.
(I128) Hozzáférés-jogosultságok ellenőrzése

- személyi hozzárendelések meghatározott (bizalmas) adatokkal végzendő input/output műveletekhez,
- többlépcsős ellenőrzési lehetőségek kihasználására (pl. egy adatbázisba való bejutásnál),
- rejtjelezés alkalmazása az azonosítási, hitelesítési folyamatokban,
- restriktív előbeállítások ("default") a hozzáférési jogosultságok vonatkozásában (például újonnan készített adatállományok harmadik személyek általi használata).

Ebben a csoportban felsorolt intézkedések a következő fenyegető tényezők hatását mérséklik:

- (F14)-(F16), (F25) - a környezeti infrastruktúra területén,
- (F82) - a dokumentumok területén,
- (F88) - a szoftver területén,
- (F105)-(F113) - az adatok területén.

9.8. Biztonsági intézkedések a kommunikáció védelmében

(I129) Az adatátviteli vezetékek és a kommunikációs kapcsolatok védelme észrevétlen bejutástól (például nehezen hozzáférhető kábelcsatornák, ellenőrizhető nyíltszíni vezetések révén).
(I130) Védelem egyes károk kihatásai ellen (tűz, víz) a kábelkoncentráció kerülésével, redundáns irányokkal, illetve a közüzemi kommunikációs kapcsolatok redundanciájával (például több X.25 csatlakozással).
(I131) A kommunikáló felek, valamint egy-egy üzenet küldőjének azonosítása és hitelesítése.
(I132) Erőforrások hálózaton keresztül való hozzáférésének ellenőrzése.
(I133) Az adatforgalom jellemzői, valamint az adattartalom, vagy annak részei bizalmasságának védelme.
(I134) Üzenet, illetve üzenetfolyam sértetlenségének védelme.
(I135) Az üzenet forrásának és az üzenet kézbesülésének bizonyítható igazolása.
(I136) Rejtjelezés.
(I137) Digitális aláírás.
(I138) Hozzáférés védelmi mechanizmusok.
(I139) Adatsértetlenséget védő mechanizmusok.
(I140) Hitelesítési információ cseréjét támogató mechanizmusok.
(I141) Forgalom kitöltés.
(I142) Útvonal-kiválasztás ellenőrzése.
(I143) Azonosítás, hitelesítés támogatása a külső hozzáférés mechanizmusával (pl. modem visszahívás).
(I144) Védelmi eljárások kommunikációs hálózatba való csatlakozásnál, például:

- kapcsolatok korlátozása fix kapcsolatokra, kimenő hívásokra, bejövő hívásokra
- zárt felhasználói csoportok bevezetése.

(I145) Biztonsági szempontok figyelembevétele helyi hálózatokban a topológia (például gyűrű, busz, csillag), az átviteli eszközök (például rézkábel, koaxiális kábel, optikai kábel), valamint az eljárások kiválasztásánál (pl. védelem új állomások észrevétlen csatlakozása, az átvitt adatok lehallgatása, stb. ellen).
(I146) A hálózati rendszerszoftver védelme manipulációk ellen (például a központi szerverről történő töltéssel).
(I147) A helyi és külső hálózat közötti átmenet logikai kontrollja, például az üzenetek szűrésével a kapcsolódó számítógépnél ("gateway").
(I148) Egyes részek kiesése vagy túlterhelése elleni védelem a hálózat konfigurációja és igazgatása révén:

- redundáns készülékek (fájlszerverek),
- dinamikus átkonfigurálás,
- osztott hálózatvezérlés,
- önálló részhálózatok,
- forgalmazás-mérések (terhelésfigyelés).

(I149) A biztonsági funkciók megbízhatóságát garantáló eszközök bevezetése:

- biztonsági címkék,
- biztonsági vonatkozású események detektálása,
- biztonsági vonatkozású események naplózása,
- automatikus biztonsági intézkedések.

Ebben a csoportban felsorolt intézkedések a következő fenyegető tényezők hatását mérséklik:

- (F27), (F28) - a környezeti infrastruktúra területén,
- (F88), (F89), (F91), (F92) - a szoftver területén

9.9. Biztonsági intézkedések a személyek védelmében

(I150) Ergonómiailag korrekt munkahelyek kialakítása (például a zajt, a világítást, az ülőhelyeket illetően).
(I151) A motiváció fenntartása.
(I152) Olyan munkahelyi szervezet, amely stresszmentes munkavégzést tesz lehetővé.
(I153) Az illetékességek rögzítése különféle szabályok kiadására, aktualizálására, betartásuk ellenőrzésére és az érintettek körének kijelölésére vonatkozóan.
(I154) Informatikai alapkiképzés valamennyi felhasználó számára.
(I155) A felhasználó bevezetése a kezelésbe, feladataira nézve.
(I156) Szakmai továbbképzés.
(I157) A biztonságtudat kialakítása és megtartása.
(I158) Egyéni bevezetések biztonsági kérdésekbe a mindenkori feladatkört illetően.
(I159) Kioktatás a jogi helyzetről, az érvényes szabályozásokról.
(I160) Kezelési utasítások kiadása az informatikai alkalmazásokhoz (például bevitel formái, paraméterek általi vezérlés, reakciók a hibajelekre, a használandó adathordozók, startidőpontok stb.).
(I161) A rendszerkezelésre vonatkozó előírások, (például manuális naplóvezetés, felügyeleti feladatok stb.).

(I162) Biztonságspecifikus előírások az alábbiakra:
- reakció akut biztonsági sérelmek gyanúja esetén (például vírusfertőzés),
- a felfedezett káresetek jegyzőkönyvezése,
- megelőző intézkedések megvalósítása stb.

(I163) A személyek és személyek csoportjainak hozzárendelése a számítógépekhez és hálózatokhoz szerepeik alapján.
(I164) Távozó (kilépő, más munkakörbe kerülő) személyektől
- jogosultságok, jelszavak visszavonása, az általa ismertek megváltoztatása,
- dokumentumok visszavétele,
- ismeretei átadásának (utódlásának) megszervezése.

Ebben a csoportban felsorolt intézkedések a következő fenyegető tényezők hatását mérséklik:

- (F14)-(F25) - a környezeti infrastruktúra területén,
- (F38)-(F49) - a hardver területén,
- (F53)-(F56), (F67)-(F70) - az adathordozók területén,
- (F80)-(F84) - a dokumentumok területén,
- (F87)-(F99) - a szoftver területén,
- (F105)-(F112) - az adatok területén,
- (F114)-(F118) - a kommunikáció területén

X.
Üzemeltetés biztonsági szabályai

10.1. Üzemeltetési eljárásrend

Az informatikai rendszerek üzemeltetésével kapcsolatos általános védelmi előírások
Az Informatikai rendszer eszközeit az üzemeltetési előírásoknak megfelelően kell használni.

A rendeltetésszerű használattól eltérő üzemeltetésből bekövetkező meghibásodás esetén a Hivatal vezetője (jegyző) anyagi kártérítést rendelhet el.
A kártérítés alapja külső, független szakszerviz szakvéleménye és az Informatikai felelős jelentése.

Az informatikai rendszer eszközeinek használatára vonatkozó általános szabályok:
- Az eszközökön és a kiegészítő berendezéseken semmilyen tárgy (papír, virág, stb.) nem tartható;
- Az eszközökön és azok közvetlen közelében mindennemű gyúlékony anyagot (papír, műanyag, stb.) TILOS tárolni!
- Az eszközök szellőzőnyílásait eltorlaszolni TILOS!

A Hivatal minden számítógépes munkahelyének rendelkeznie kell hálózati/gépi jelszóval.
A jelszórendszert az Informatikai vezető dolgozza ki a Jelszókezelés szabályai szerint, és ő telepíti a számítógépes munkahelyekre.
A jelszó titkos!
A jelszó átadásából eredő mindennemű kár és hátrány, a jelszó átadóját terheli.

Az Informatikai felelős az alábbi nyilvántartásokat vezeti:
- Informatikai eszközök – felhasználó munkahely;
- Szoftver- és licencnyilvántartások;
- Hálózati/gépi jelszórendszer;
- Szoftver jogosultságok;
- Mentési rend;
- Üzemeltetési Napló
- Rendszerfelelősök;
- Internet jogosultságok – postafiókok – azonosítók.

A nyilvántartásokat az Adatvédelmi felelős –az Informatikai felelős szakmai bevonásával- félévenként ellenőrzi és az ellenőrzésről feljegyzést készít a jegyző részére.

10.2. Naplózás

A naplózást, a sértetlenség és bizalmasság szempontjából fokozott védelmi szintbe sorolt minden informatikai eszközön és az azokon futtatott alkalmazásokon engedélyezni kell, az alábbi szabályok szerint:
- naplózza a rendszer leállását, leállítását és újraindítását;

- naplózza a rendszeróra állítását,
- naplózza a rendszerben fellépő hardver hibákat;
- naplózza az üzemeltetői bejelentkezést vagy sikertelen bejelentkezési kísérleteket.

10.3. Mentési rend

Mentés

A hivatalnak az informatikai rendszerek szoftverelemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan mentési renddel és biztonsági mentésekkel kell rendelkeznie, amelyek biztosítják, hogy az érintett eljárási cselekmény biztonsági osztályba sorolásától függő helyreállítási időn belül az informatikai rendszer helyreállítható legyen.

Az mentési rend meghatározza a mentések típusát, módját, a visszatöltési és helyreállítási teszteket, valamint eljárásokat.

A mentéseket azok tartalmától függően kockázati szempontból elkülönítetten, és biztonsági osztályba sorolástól függően indokolt esetben tűzbiztos módon kell tárolni.

A biztonsági őrzés során az adatok elhelyezését és tárolását olyan rendszerességgel, módon és dokumentáltsággal kell végezni, amely a nyilvántartást vezető informatikai célrendszer teljes megsemmisülése esetén is lehetővé teszi a nyilvántartás azonos funkcionalitású, és lehetőség szerinti legteljesebb adattartalmú újbóli kialakítását.

A biztonsági őrzés során gondoskodni kell arról, hogy az adatokat az arra jogosult személyen (adatkezelőn és adatfeldolgozón) kívül más ne ismerhesse meg, valamint biztosítani kell az adatok jogosulatlan személy általi megsemmisítése, megváltoztatása vagy hozzáférhetetlenné tétele elleni védelmét mind a szervezeten belülről, mind a szervezeten kívülről jövő informatikai támadások esetén.

A mentések célja

A szerverek meghibásodásakor bekövetkező esetleges adatvesztés után, a rendszerfájlok és meghatározott felhasználói adatok visszaállíthatósága, az előző napi állapotnak megfelelően.

Véletlen felhasználói törlés esetén a törölt fájlok egy előző állapotának visszaállítása.

Mentési kategóriák

- Rendszeradatok: azon fájlok, melyek a szerveren lévő operációs rendszer gyors visszaállítását teszik lehetővé.
- Felhasználói adatok: azon adatok, dokumentumok melyeket a felhasználók a fájlszerveren vagy a lokális gépen tárolnak.

Mentések periódusa

- A rendszeradatok előző állapotát a rendszer megváltoztatása esetén kézi indítással kell menteni.
- A fájlszerveren tárolt felhasználói adatokat minden munkanapon, ütemezett feladatként éjszakai időszakában automatikusan menteni kell.
- A mentést tömörített állapotban kell tárolni. A tömörített állomány neve tartalmazza a tömörítés dátumát.

A mentések mechanizmusa

- A központi mentésbe bevonásra kerül minden hálózatra kötött munkaállomás gép dokumentum-állománya, és azok a szakalkalmazás adatbázisok, amelyek támogatják a hálózatos felhasználást (KataWin, Számadó).
- A mentést tartalmazó tömörített állomány a szerveren jön létre, az aktuális dátummal. A mentést célszoftver végzi.
- A szerveren a korábbi napi mentések megtalálhatók mindaddig, amíg a szerver kapacitása ezt lehetővé teszi.
- A régebbi napi mentésekből a rendszergazda szükség esetén manuálisan úgy töröl állományokat, hogy a heti, illetve havi mentések megmaradjanak.
- A havi mentéseknek és a rendszeradatok akkori állapotának egy merevlemezre mentett másolatát –tűzvédelmi okokból- páncélszekrényben kell tárolni.
- A mentés típusa növekményes (inkrementális), az utolsó mentéshez képest a megváltozott adatállományok kerülnek mentésre.
- A lokális szakalkalmazások mentéséről az alkalmazás felelőse egyedileg gondoskodik.

Metés naplózása

A rendszergazda –a napi automatikus mentéseken kívü – minden mentési eseményt rögzít a szerver naplóban.

Korábbi adatállomány visszaállítása a mentésekből

Ha a felhasználó egy adatállományának korábbi változatát kéri visszaállítani, akkor ezt a rendszergazda a dátum szerinti napi, heti vagy havi tömörített mentés kibontásával kell megoldja.

10.4. Adathordozók védelme, kezelése, tárolása, selejtezése

A mentésre használt adathordozókkal kapcsolatban az alábbi kezelési, tárolási szabályokat kell betartani:

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni (erről nyilvántartást kell vezetni);
- a nyilvántartásban az azonosító adaton kívül a felírás és megőrzés dátumát, a védettség tényét, a jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell feltüntetni;
- a használni kívánt adathordozót (floppy disk, CD-ROM, DVD-ROM stb.) a tárolásra kijelölt helyről kell kivenni és oda kell vissza is helyezni;
- az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet;
- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek;
- adathordozót más intézménynek átadni csak az adatvédelmi felelős engedélyével lehet;
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a felelős vezető (jegyző) határozza meg;
- az adathordozókat félévenként ellenőrizni és tisztítani kell;

- olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell.

Selejtezendő az adathordozó, ha:

- fizikailag sérült, javíthatatlan,
- gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott),
- a kapacitása a névleges értékének 75%-a alá csökkent,
- véglegesen elhasználódott.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni, bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.
A selejtezést a Selejtezési Szabályzatnak és a hivatal Iratkezelési Szabályzatának megfelelően kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni.
Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

XI.
Záró rendelkezések

Jelen szabályzat hatályba lépésével a 2007. január 1-én módosított és jóváhagyott Számítástechnikai Adatvédelmi Szabályzatban található mellékletek a továbbiakban is irányadóak.

Elosztási lista:

A szabályzatot kapják:
- polgármester
- alpolgármester
- jegyző
- aljegyző
- csoportvezetők

A Polgármesteri Hivatal informatikai adatvédelmével megbízott személyek:

Hivatali Adatvédelmi felelős: Böröndyné Nagy Anikó aljegyző

Informatikai felelős: Kluik Tamás informatikus

Rendszerfelelősök: -

Répcelak Város Önkormányzata Informatikai Biztonsági Szabályzatának 2011. március 1-től hatályos módosítása:

I. A szabályzat 5.1. és 5.2. pontja helyébe az alábbi lép:

V.

Adatvagyonleltár

5.1. Szoftverek, szakalkalmazások

LINUX SME 8.0	1
Microsoft Windows XP	14
Microsoft Windows 7	3
Microsoft Office	13
Libreoffice	2
Openoffice	2

Számadó	Főkönyvi könyvelés	Hálózatos/Központi
K11	Költségvetés és beszámoló készítő	Szólógép/Egyedi
Onkadó	Adónyilvántartó	Szólógép/Egyedi
Mérleg	Mérleg készítő	Szólógép/Egyedi
Házi pénztár	Házi pénztár	Szólógép/Egyedi
KataWin	Ingatlanvagyon kataszter	Hálózatos/Központi
OTP Ügyfélterminál	Banki utalások	Szólógép/Egyedi
Vizuál Regiszter	Népességnyilvántartás	Szólógép/Egyedi
Winszoc	Szociális segélyezés	Szólógép/Egyedi
Okmányirodai rendszerek		Hálózatos/Központi
ASZA rendszer	Anyakönyvi rendszer	Hálózatos/Központi
Iktatás (E-Iktat)	Iktatás, iratkezelés	Hálózatos/Központi

5.2. Hardverek, hálózat

File szerver (SME): Intel P4	1
PC számítógép konfigurációk (monitorral)	17
Tintasugaras nyomtatók	4
Lézernyomtatók	8
Mátrixnyomtatók	3
Router (Wifi 4 portos)	1
Switch (24 portos)	1
Switch (5 portos)	2
Switch (8 portos)	2

II. A szabályzat az ÁSZ ellenőrzés kapcsán tett észrevételének megfelelően az alábbi intézkedésekkel egészül ki::

Az ÁSZ vizsgálatának eredményeként a pénzügyi-számviteli feladatoknál alkalmazott informatikai rendszerekkel kapcsolatban az alábbi javító intézkedéseket vette szabályzatba a Hivatal:

1.1 Észrevétel: A pénzügyi-számviteli rendszerek hozzáférési jogosultságokra vonatkozó eljárásrendjében rendelkezzenek a jogosultság visszavonásáról is
Intézkedés: A SZÁMADÓ nevű pénzügyi-számviteli szoftver hálózatos környezetben fut, ehhez való hozzáférési jogosultsága csak a jegyző által kinevezett és engedélyezett dolgozóknak van. A jogosultság jelszóhoz kötött, ami havonta – a jelszó biztonsági szabályok szerint – megváltoztatásra kerül. Az észrevételezett jogosultság-visszavonást úgy szabályozta az IBSZ, hogy az időközben nem jogosulttá váló felhasználók jelszava nem került megújításra, azaz lejárt, így az alkalmazáshoz való hozzáférésük is hatályát vesztette.

1.2 Észrevétel: Az informatikai területen tiltsák meg a pénzügyi-számviteli szoftverekhez kapcsolódóan a külső fejlesztők hozzáférését az éles rendszerekhez.
Intézkedés: Az észrevétel nem igényelt érdemi intézkedést, ugyanis központi menedzselésű és fejlesztésű államigazgatási alkalmazásról van szó, melyhez külső fejlesztő nem fér hozzá. A Hivatal belső hálózatán futó alkalmazás egyrészt jelszavas jogosultsághoz kötött, másrészt nem tartalmazza a fejlesztéshez szükséges forráskódokat, így a programba való külső beavatkozást kizárt.

1.3 Észrevétel: Tegyék lehetővé a pénzügyi-számviteli rendszerből ellenőrzési listák lekérhetőségét.

Intézkedés: Az észrevétel nem igényelt érdemi intézkedést, ugyanis központi menedzselésű és fejlesztésű államigazgatási alkalmazásról van szó, melyben a pénzügyi-számviteli előírásoknak megfelelő és a fejlesztést végző cég által deklarált és leprogramozott lekérdezési, ellenőrzési listák érhetők el. A program funkcionalitására (pl. új ellenőrzési lista létrehozása) nincs ráhatása az azt használó pénzügyi-számviteli feladatot ellátóknak.

1.4 Észrevétel: Szabályozzák a pénzügyi-számviteli szoftver-változások ellenőrzésére, tesztelésére vonatkozó eljárásokat.
Intézkedés: Az észrevétel nem igényelt érdemi intézkedést, ugyanis központi menedzselésű és fejlesztésű államigazgatási alkalmazásról van szó, melynek verzió- és jogszabálykövetése valamint ezek tesztelése az államilag megbízott fejlesztést végző cég feladata. A mindenkori szoftverváltozások központi internetes felületről érhetők el (eAdat), melyről értesítést kap a hivatal. Az internetes felületen csak az aktuális verzió érhető el, így verzióeltérés (pl. régebbi verzió téves visszatöltése) kizárható, illetve hatékonyan orvosolható.

1.5 Észrevétel: A pénzügyi-számviteli szoftver mentési eljárások esetében a felelősség is kerüljön szabályozásra.

Intézkedés: A pénzügyi-számviteli rendszer által előállított adatok mentésével külső céget bízott meg a Hivatal. A cég felelősségét a biztonsági szabályzatban deklaráltuk az ÁSZ észrevétele értelmében. Erről a céget a vonatkozó szabályzati pontok beemelésével értesítettük.

Az ÁSZ kérte a Hivatal jegyzőjét, hogy az informatikai rendszerek folyamatos működésének biztosítása érdekében gondoskodjon:

a.) A pénzügyi-számviteli feladatok informatikai ellátásánál a főkönyvi könyvelési rendszerben tárolt hozzáférési jogosultságok ellenőrizhetőségéről.
Intézkedés: fenti feladatokra a SZÁMADÓ nevű központi fejlesztésű szoftvert kötelező használni. A program napjaink informatikai fejlettségéhez képest elavult, kb. 20 éves technológián alapul (DOS-os, karakteres felületű) jogosultsági szinteket nem tartalmaz. A jegyző hozzáférési jogosultság-ellenőrzési hatásköre a szoftvert használók személyére terjed ki, az általa kinevezett, a szoftverhez hozzáférő szakfeladatot ellátó személy kap jogosultságot az 1.1 ÁSZ észrevétel szerinti formában. Ezen jogosultságok kiosztása és menedzselése a hálózati rendszeradminisztrátor (informatikus) feladata.

b.) A pénzügyi-számviteli szoftver elemeire vonatkozó változáskezelési eljárásoknak és a változáskezelési eljárások ellenőrzésének, tesztelésének dokumentálásáról.

Intézkedés: A pénzügyi-számviteli szoftver változáskezelési eljárása nem más, mint a szoftver frissítése, verzióváltása. A program frissítése központilag történik, az ÁSZ 1.4 Észrevételre hozott intézkedés alapján (eAdat). A mindenkori szoftverváltozások központi internetes felületről érhetők el (eAdat), melyről értesítést kap a hivatal. Az internetes felületen csak az aktuális verzió érhető el, így verzióeltérés (pl. régebbi verzió téves visszatöltése) kizárható, illetve hatékonyan orvosolható. A verziófrissítést a hálózati rendszeradminisztrátor (informatikus) végzi, minden esetben a verzióváltáshoz mellékelt telepítési útmutató alapján.

c.) A mentett állományok helyreállíthatóságának ellenőrzéséről.

Intézkedés: A mentett állományok helyreállíthatóságára és az adatmentés folyamatának menedzselésére a Hivatal külsős céget (Blue System Kft.) bízott meg, mely élő szerződés alapján ellátja a fenti feladatokat.

Répcelak, 2011. február 27.

VÁROSI POLGÁRMESTERI HIVATAL * RÉPCELAK *