POMÁZ VÁROS POLGÁRMESTERI HIVATAL INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Az Informatikai Biztonsági Szabályzat (a továbbiakban: Szabályzat) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. Törvény (a továbbiakban: Info tv.) 24.§ (3) bekezdése alapján Pomáz Város Polgármesteri Hivatalra (továbbiakban: Hivatal) vonatkozóan általános érvénnyel meghatározza az információ technológiai (a továbbiakban: IT) rendszerekkel és IT eszközökkel kapcsolatos üzemeltetési-, adatvédelmi- és állagmegóvási szabályokat, valamint intézkedéseket.

I.
A Szabályzat célja

A Szabályzat kiadásának célja, hogy a Hivatal tulajdonában lévő, illetve az általa üzemeltetett IT rendszerek védelmét, valamint az IT rendszerekkel kezelt adatok bizalmasságát, hitelességét, sértetlenségét, rendelkezésre állását a fenyegető veszélyekkel szemben – a Szabályzat által előírt intézkedésekkel, szabályozással – biztosítsa.

II.
A Szabályzat tárgyi hatálya

A Szabályzat rendelkezései az adatokra és azok hordozóinak végleges megsemmisítéséig, a közlésre szánt adatoknak a felhasználásáig, a személyhez fűződő és vagyoni jogokra, a számítástechnikai berendezések, azok környezete, működésük biztonsága és a dokumentációk, a mágneses adathordozók hiánytalan meglétére, a rajtuk tárolt programok és adatok használhatóságára, a számítástechnikával összefüggő műszerek, eszközök meglétére és használhatóságára, a számítástechnikai berendezésekhez tartozó okmányokra, programokra és azok dokumentációira, az alkalmazott biztonsági intézkedésekre, azok terveire, tartalmi előírásaira és eljárási szabályaira terjed ki.

III.
A Szabályzat személyi hatálya

1. A Szabályzat hatálya kiterjed a Hivatal minden olyan munkatársára (ideértve a köztisztviselőket, az ügykezelőket, a fizikai alkalmazottakat és a Munka Törvénykönyve alapján foglalkoztatottakat), akik a munkavégzés, feladat-ellátás során IT eszközökkel, valamint az általuk kezelt adatokkal kapcsolatba kerülnek, ezekkel az eszközökkel, adatokkal munkát végeznek.
2. A Hivatal informatikai rendszerével, szolgáltatásaival polgári jogi jogviszony alapján vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre a velük kötött szerződésben rögzített mértékben, illetve titoktartási nyilatkozat alapján.

IV.
Általános üzemeltetési szabályok

1. Hálózati azonosítás, hozzáférés

1.1 Üzemeltetési fogalmak meghatározása

- **Hozzáférés (account)** – a felhasználó azonosítója adott rendszerben. Az account-ot meghatározza: felhasználónév és a jelszó.
- **Felhasználó (user)** – az a személy, aki az adott rendszer használatára jogosított account-ot kapott
- **Bejelentkezés (logon)** – az a folyamat, melyben a felhasználó account adatait egy rendszer számára érvényesítés céljából megadja
- **Tartomány (domain vagy körzet)** – rendszeradminisztrációs egység, ahol az account definiálva van
- **Házirend (policy)** – az adott rendszer használatát szabályzó előírások összessége, mely vonatkozhat felhasználóra és számítógépre egyaránt
- **Felhasználói név (user name)** – az account része, mely a felhasználót az adott rendszerben egyedileg azonosítja
- **Jelszó (password)** – a felhasználó által választott betű és/vagy számkombináció, mely a felhasználót igazolja. A házirendben meghatározott szabályoknak eleget kell tegyen
- **Erőforrás (resource)** – egy informatikai eszköz szolgáltatása, melyet feladatok elvégzésére fel lehet használni (pl. lemez terület kiszolgálón, hálózati nyomtató, munkaállomás processzorideje, stb.)
- **Alkalmazásgazda** – Az a személy aki adott alkalmazás fölött az összes hozzáférési jogot gyakorolja

2. Megosztási mappákhoz való hozzáférés

Felhasználói azonosítás az a folyamat, amikor a rendszer a felhasználó által megadott account információ alapján eldönti, hogy az helyes-e, az azonosítást kérő személy rendelkezik-e érvényes account-tal.

Azonosítás két szinten történhet.

- Hálózati szinten
  A felhasználó egy hálózati rendszerbe vagy egy kiszolgálóra jelentkezik be.
- Alkalmazás szintjén
  Ha a felhasználó által használni kívánt alkalmazás (program) saját hitelesítési rendszerrel rendelkezik, akkor az ott érvényes felhasználói paraméterekkel jelentkezik be.

2.1. Windows hálózati bejelentkezés

A Hivatal által használt hálózati rendszerben az azonosítás olyan account információ felhasználásával történik, melynek részei

- a felhasználói név,

- jelszó,

melyek együttesen érvényesek. A felhasználói neveket meghatározott szabály szerint, a rendszergazda hozza létre az aljegyző utasítására.

2.2. Alkalmazás szintű bejelentkezés

Ha egy alkalmazás futtatásához vagy annak adatainak eléréséhez felhasználói azonosításra van szükség, és az alkalmazás önálló felhasználó-kezeléssel rendelkezik, akkor alkalmazás szintű bejelentkezésre van szükség.
Ebben az esetben a program használatához a hálózatitól eltérő account-ot kell beszerezni az alkalmazás gazdájától.

3. Hozzáférés igénylése

A Polgármesteri Hivatalban a hálózati jogosultságok kezelése a SAMBA szerveren keresztül történik.

3.1. Hálózati kiszolgáló

A hozzáférést minden esetben igénylőlap (adatlap) benyújtásával kell megkérni.

Az igénynek tartalmaznia kell:

- a felhasználó pontos adatait
- a szükséges szolgáltatásokat és jogosítások szintjét

Az igénylőlapot az aljegyzőnek kell címezni jóváhagyásra. Jóváhagyás nélküli igényeket a rendszergazda nem teljesíti.

3.2. Alkalmazások, felhasználói rendszerek

A hozzáférési kérelem írásban történik az alkalmazásgazda felé. Mivel az alkalmazásgazda és az alkalmazás által kezelt adatok felelőse a legtöbb esetben nem azonos, ezért az alkalmazásgazda felé továbbított igénylő dokumentumnak tartalmaznia kell:

- az alkalmazás nevét
- a hozzáférés szintjét (írás, olvasás, törlés, stb.)
- az adatok felelősének hozzájárulását

4. Account átvétele

1. az elkészült account kézbesítéséről az rendszergazda gondoskodik
2. az account átadása kizárólag annak tulajdonosának történhet

Az account kézbesítésének módjai:

A felhasználó érdekeinek védelmében az account átvételekor egy jelszó kerül átadásra, mely nem megváltoztatandó. Alkalmazások felhasználói számára a jelszócsere ajánlott (amennyiben lehetséges).

5. Az account felhasználási feltételei

- a személyre szólóan kiadott jelszót a felhasználó köteles titokban tartani. Másnak átadni, leírni, vagy egyéb formában rögzíteni tilos!
- hivatali vezető beosztottját jelszavának átadására nem utasíthatja.
- a Hivatal hálózatában, alkalmazásaiban, rendszereiben használt jelszavak nyilvános hálózatban való (Internet) használata nem javasolt.
- a felhasználó nem hagyhatja felügyelet nélkül azt a munkaállomást/alkalmazást, melyre bejelentkezett.
- ha munkaállomástól/alkalmazástól eltávozik, köteles azt a munkaállomás zárolásával (Lock Workstation) védeni.
- hosszabb időtartamra való távozás esetén (pl. munkanap/műszak vége) az alkalmazásból és a munkaállomásról is ki kell jelentkezni, a munkaállomást ki kell kapcsolni, kivétel ha az rendszergazda másképpen nem rendelkezik.

6. Hozzáférés korlátozása (account zárolása)

A biztonsági előírások és a Hivatal érdekei megkövetelik, hogy visszaélések és azok gyanúja esetén a felhasználó rendszerhez/hálózathoz/alkalmazáshoz való hozzáférése korlátozva legyen. Korlátozások életbe léphetnek automatikusan, vagy a rendszergazda kezdeményezésére az aljegyző jóváhagyásával.

6.1. Manuális korlátozások

- account jogosulatlan használatakor
- jogosultságokkal való visszaélés, károkozás esetén
- a munkavégzésre irányuló jogviszony megszűnésekor
- a köztisztviselő, egyéb foglalkoztatott felettesének indokolt kérése alapján

Az aljegyző által kezdeményezett korlátozások feloldása az esemény tisztázódása után lehetséges, jegyzői jóváhagyással.

7. Felelősség

- a köztisztviselő, egyéb foglalkoztatott felelősséggel tartozik a személyre szólóan átvett account-ért,
- a kitudódott jelszó illetéktelen felhasználásából eredő kár és felelősség az account tulajdonosát terheli,
- a jelszó elfelejtéséből eredő károkért, munkakiesésért a jelszó-visszaállítás teljes időtartama alatt a felhasználó a felelős,
- a Szabályzatba ütköző bármely magatartást tanúsító, valamint a szándékos, vagy az elvárható gondosságot elmulasztó tevékenységgel kárt okozó felhasználó, az előidézett vagyoni és nem vagyoni károkért kártérítési felelősséggel tartozik.

8. Szankciók

Az account felhasználási feltételeinek, valamint a jelen Szabályzat valamely rendelkezésének sorozatos megszegői ellen a jegyző fegyelmi felelősségre vonást

kezdeményezhet a Kttv. alapján. Amennyiben a felhasználónak a Hivatal IT rendszereinek használata során kifejtett tevékenysége zavarja, veszélyezteti vagy bármilyen módon akadályozza az IT rendszerek rendeltetésszerű használatát, vagy e tevékenysége a Hivatal valamely szabályzatát sérti, akkor a rendszergazda a felhasználó hozzáférési jogosultságait haladéktalanul, határozatlan időre felfüggesztheti további rendelkezésig, egyúttal a hozzáférési jogosultságot jóváhagyó aljegyző felé köteles jelezni a szabálytalan használatot. A további rendelkezés joga a jegyző hatáskörébe tartozik.

9. Naplózás

A védelemi módszerekhez sorolható még a naplózás (audit) rendszere, amely ugyan közvetlenül nem alkalmas a hozzáférés megakadályozására, de az utólagos ellenőrzések miatt visszatartó, s később bizonyító hatása van.
A megbízható működéssel kapcsolatos eseményekről (rendszerindítás/leállás, nagyobb üzemzavarok, alap- és felhasználói szoftverekkel kapcsolatos, a megbízható működést érintő események) gépi, illetve manuális biztonsági naplózásokat kell végezni.
A szerverek naplóállományaihoz csak az rendszergazda férhet hozzá, míg a kitüntetett alkalmazások naplóállományait csak az adminisztrátorok láthatják és elemezhetik.

10. Kiemelt fontosságú adatok

A Hivatali munkavégzés során használt számítógépek kiemelt adatait az alapján lehet megállapítani, hogy az egyes gép, mely alkalmazási területen van jelen. Általánosságban megállapítható, hogy az összes Hivatali számítógépen tárolt Microsoft Office dokumentumok, legyen az Word, Excel vagy PowerPoint prezentáció, védett anyagnak minősül. Azaz amennyiben az említett dokumentumok valamelyike nem elérhető a felhasználó számára, az adatvesztésnek tekinthető.
Védett adatnak minősül továbbá a felhasználói levelezés is, mely nemcsak a fogadott leveleket érinti, hanem a felhasználó által kiküldött leveleket is.
Ezek alapján a következő fájltípusokat tekinthetjük védett adatoknak:

- .doc, .xls, .ppt, .pps
- .pdf
- .eml, .dat, .pst, .ost, .pad

Továbbá vannak olyan speciális felhasználói szoftverek, melyek a Hivatali munkavégzés egy-egy speciális területén kapnak szerepet. A Magyar Államkincstár által adott kötelezően használandó szoftverek illetve a Hivatal testületi ülését támogató rendszerek. A fent említett rendszerek szoftverek által használt védett adatok kiterjesztése: .dbf; .dat; .html; .xml;.mp3.

V.
Az IT eszközök védelme

1.1 Rendészeti védelem

A Polgármesteri Hivatal területén a stratégiai fontosságú hardver eszközöket (szerverek, routerek, telefonközpont) külön zárható helyiségben kell elhelyezni. Erre a külön elhelyezésre szolgál a Hivatalban a rendszergazda által működtetett szerver szoba (a továbbiakban: szerver szoba), valamint azok a Hivatali helyiségek, amelyekben azok az adatszerverek kerültek elhelyezésre, amelyek a Hivatal működése során használatosak.

A szerver szobába, valamint az adatszerverek Hivatali helyiségeibe csak az arra illetékes személyek léphetnek be.

A gépterem, valamint az adatszerverek Hivatali helyiségeinek ajtaját külön kulccsal zárni kell. Kulcsot (kulcsokat) csak az arra illetékes, engedéllyel rendelkező személyek tarthatják maguknál. A géptermek kulcsának egy példányát lezárt borítékban jól őrzött helyen kell elhelyezni (páncélszekrényben, annak hiányában pénzkazettában vagy biztonságosan zárható szekrényben), a rendszergazda által működtetett gépterem esetében a Jegyzői Titkárságon. A boríték esetleges felbontását jegyzőkönyvben rögzíteni kell.

1.2. A felhasználói szintű védelmi szabályok

Az IT eszközök rendeltetésszerű működéséért a használatra kijelölt személy (a továbbiakban: felhasználó) a felelős.
A felhasználó köteles a rábízott eszközt a jó gazda gondosságával kezelni, állagmegóvással működtetni, valamint a szándékos és vétlen károkozást elkerülni.
Az eszközök burkolatát felnyitni, azon bármilyen javítást végezni csak az arra kijelölt szakembernek (rendszergazda) vagy az általa meghatalmazott személynek van joga.
A felhasználó köteles a részére átadott eszköz üzemeltetési leírását, valamint a hozzá tartozó floppy, CD és DVD adathordozókat az eszköz közelében elhelyezni, esetleges javítás esetén a javítást végző szakember részére rendelkezésre bocsátani, amennyiben ezekre a felhasználónak továbbiakban nincs szüksége a rendszergazdának megőrzésre átadni. Ez alól kivételt képez a licence konstrukcióban vásárolt szoftver, szoftverek tárolása, biztosítása. Ezen szoftverek a javítást, karbantartást végző szakemberek részére rendelkezésre állnak.
A eszközök működése során tapasztalt működési zavarokat a felhasználó köteles haladéktalanul a e-mailen vagy a hibabejelentő rendszeren a rendszergazdát értesíteni. A hibás eszközzel a hiba elhárításáig további munkavégzés nem folytatható.

1.3. Az rendszerszintű védelem

A védelmi felelősök feladatai

a) **Az aljegyző feladatai:**

- meghatározza a védett adatok körét,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- az adatvédelmi feladatok ismertetése,
- ellenőrzi a szoftverek használatának jogszerűségét.

b) **Rendszergazda feladatai:**

- a jelen Szabályzat kezelése, naprakészen tartása, módosítások átvezetése,
- a saját külön feladatkörébe tartozó rendszerek felügyelete,
- felel az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
- a védelmi eszközök működésének folyamatos ellenőrzése,
- felel a Hivatali IT hardver eszközeinek karbantartásáért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos vírusvédelemről
- vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- ellenőri tevékenységét adminisztrálja.

A rendszergazda ellenőri feladatai

- évente egy alkalommal részletesen ellenőrzi a jelen Szabályzat előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

A rendszergazda jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a jegyzőnél,

- bármely érintett osztályon jogosult ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

1.4. Illetéktelen felhasználás

A Hivatal tulajdonában lévő IT eszközök használata külső személyek számára csak a jegyző által meghatározott engedéllyel és nyomon követhető módon (átadás-átvételi nyilatkozat kíséretében) lehetséges.
Eszközöket javításra átadni csak átvételi elismervény ellenében szabad.
Az értékesítés, selejtezés céljából átadott eszközökön tárolt adatok védelméről az eszközt használó szervezeti egység vezetője gondoskodik.

1.5. Hardver eszközök beszerzése, selejtezése

Számítástechnikai eszközök beszerzése és selejtezése csak az aljegyző és a rendszergazda által jóváhagyott paraméterek alapján történhet. Selejtezéshez a rendszergazda írásos javaslata szükséges, melyből kiderül a selejtezés oka, az eszköz állapota illetve becsült értéke. A használt eszköz becsült értékének a megállapításakor a piaci értéke vagy a könyv szerinti értéke közül a magasabb összeget kell figyelembe venni.

1.6. Üzemen kívüli eszközök tárolása

Az ideiglenesen üzemen kívüli számítástechnikai eszközök tárolása a szerver szobában történik, illetve az erre a jegyző által kijelölt helyen. Ezen helyekre, helyekről a számítástechnikai eszközök áthelyezése, kihelyezése (üzembe állítása) a rendszergazda tudtával és belegyezésével történhet.

2. Szoftver és adatvédelem

2.1. Verziókövetés

A hivatali munkavégzés során használt szoftverek frissítése, naprakész állapota elengedhetetlen a hibamentes működés érdekében. A Hivatal több olyan szoftverrel rendelkezik, melyek a feladatellátáshoz folyamatosan frissülnek, újabb és újabb verzióval kerülnek telepítésre, a hivatali számítógépekre. Az automatikusan települő, frissülő programokkal kapcsolatban nem szükséges szabályozás az automatizmus miatt, és az említett szoftverek naprakészsége kiemelten fontos a Hivatal számára.

A nem automatikusan frissülő programok esetében a rendszergazdának egy előzetes tesztelést kell végezni a frissített szoftverre vonatkozóan, mely tesztben ellenőrzi a program hibamentes működését. Amennyiben a rendszergazda által elvégzett teszt sikeres volt, abban az esetben kerülhet a telepítésre a Hivatal rendszerébe az új verziójú szoftver.

2.2. Az adattárolók védelme

Adattároló eszköznek kell tekinteni a hajlékony-, cserélhető merevlemezeket, optikai lemezeket, kazettákat, és az elektronikusan írható-olvasható adattárolókat. Az adattárolók megóvása a Hivatal minden dolgozójának kötelezettsége. Adattárolót illetéktelen személynek átadni, még megtekintés idejére sem lehet. Az adattárolók megóvása érdekében tárolásukra egy külön vagy erre a célra kialakított helyet kell használni.

2.3. A szoftverek védelme

A Hivatalon belül csak hivatalosan beszerzett, írásbeli igazolással (számla, licence-szerződés) ellátott szoftvereket lehet használni. A szoftverekről – az eszközök nyilvántartásához hasonló módon - számítógépes nyilvántartást kell vezetni, amit a mindenkori helyzetnek megfelelően aktualizálni szükséges.
A beszerzett és használatban lévő programok védelme a Hivatal minden dolgozójának feladata. A Hivatal rendszereiben használatos alkalmazásokat, adatokat külső illetéktelen személyekkel megismertetni, azt átadni, lemásolni tilos. Az alkalmazás során a megszokottól történő eltérés esetén azonnal értesíteni kell a rendszergazdát, aki köteles a továbbiakról intézkedni. A számítástechnikai rendszerekbe, alkalmazásokba illetéktelen személynek behatolni, bármilyen idegen programot telepíteni, bemásolni tilos.
Biztosítani kell a felhasználók részére a felhasználói programok leírását. Új alkalmazás bevezetésekor biztosítani kell az alkalmazást használó munkatárs továbbképzésen történik részvételét.

2.4. Vírusvédelem

A Hivatalon belül a számítógépek vírusvédelme a F-Secure Antivírus szoftvertermékkel valósul meg. A rendszergazda kötelessége a rendszer ellenőrzése, és szükség esetén beavatkozás annak működésébe.
A felhasználó külső adathordozó használata esetén köteles azon előzetes vírusvédelmi vizsgálatot végezni.
Amennyiben a felhasználó vírusra utaló jelenséget tapasztal, köteles azt jelezni a rendszergazdának. Munkavégzés az adott eszközön csak a megfelelő és alapos vírusvédelmi átvizsgálás után lehetséges.
Nem írtható vírus esetén a rendszergazda köteles jelentést küldeni a vírusvédelmi szoftver terméktámogatási ügyfélszolgálatának, majd a legrövidebb időn belül megoldást találni a kártékony állomány eltávolítására.

Az elektronikus levelezés vírus és spam védelme szerverszinten szintén a F-Secure Antivírus szoftvertermékkel történik. Ennek felügyelete az rendszergazda feladata.

2.5. Adatvédelem, adatok mentése

Az IT rendszerekben található, illetve velük kapcsolatos adatokra a Hivatal Adatvédelmi és Adatbiztonsági Szabályzatában foglaltak vonatkoznak.
A felhasználók kötelesek az általuk kezelt rendszerek adatait a rendszerek belső mentési mechanizmusa segítségével napi rendszerességgel menteni mágneses adathordozóra. Ezen felül a rendszergazda köteles heti rendszerességgel, illetve szükség szerint mentést végezni az általuk felügyelt területekről.

Az IT rendszer kapcsolatban áll az Internet hálózattal, ezért az Internet irányába a ZyXEL ZyWALL 35 típusú hardveres tűzfal védelem került kialakításra. A tűzfal működésének felügyelete a rendszergazda feladata.

VI.
IT katasztrófahelyzetek kezelése

1. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten, megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

1.1. Környezeti infrastruktúra okozta ártalmak

Elemi csapás
- földrengés,
- árvíz,
- tűz,
- villámcsapás, stb.

Környezeti kár
- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por).

Közüzemi szolgáltatásba bekövetkező zavarok
- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

1.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás
- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás
- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

2. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

2.1. Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

2.3. A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,

- helytelen adatkezelés,
- programtesztelés elhagyása.

2.4. A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

3. Az informatikai eszközök környezetének védelme

3.1. Vagyonvédelmi előírások

- a szerverszobába történő illetéktelen behatolás tényét a jegyzőnek azonnal jelenteni kell
- az IT eszközöket csak a Hivatal arra felhatalmazott alkalmazottai használhatják,
- az IT eszközök rendeltetésszerű használatáért a felhasználó felelős.

3.2. Tűzvédelem

- a szerverszoba illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent,
- a menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell,
- a Hivatal szerverszobáiba minimum 1 db tűzoltó készüléket kell elhelyezni,
- a szerverszobában elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni,
- a nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése a rendszergazda és az vezetők feladata.).

4. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

4.1. A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

4.2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetést, karbantartást és szervizelést a rendszergazda végzi, végezteti.
A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.

Alapgép megbontását (kivéve a garanciális gépeket) csak rendszergazda vagy az általa meghatalmazott személy végezheti el.

4.3. Az informatikai feldolgozás folyamatának védelme

4.3.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- az adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.
- hozzáférési lehetőség:
    - a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá).
    - az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
    - A szerverek rendszergazda jelszavát a rendszergazda kezeli.

4.3.2. Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

4.3.3. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését. A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.
A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban a rendszergazda segítséget nyújt.

4.4. Szoftver védelem

4.4.1. Rendszerszoftver védelem

A rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

4.4.2. Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

5. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

5.1. Központi gépek

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni. A vásárolt szoftverekről biztonsági másolatot kell készíteni.

5.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal. Vírusfertőzés gyanúja esetén a rendszergazdát értesíteni kell.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
A Hivatal informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz felelőse tudtával és engedélyével szabad.

6. Ellenőrzési elvek

Az ellenőrzéseknek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.
A munkafolyamatba épített ellenőrzés során a Szabályzat rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői (vezetők) folyamatosan ellenőrzik.

A Polgármesteri Hivatal által elektronikus úton, számítógéppel készített dokumentumok biztonságos tárolásához történő hozzáférést és a különböző jogosultsági szinteket az 1. számú melléklet rögzíti.

VIII.
Záró rendelkezések

Jelen szabályzat 2012. november 1-én lép hatályba, és a 2009. november 15-én hatályba lépett informatikai biztonsági szabályzat hatályát veszti.
A szabályzat elkészítéséért és végrehajtásáért a Jegyző felelős.
A szabályzatot a Polgármesteri Hivatal valamennyi köztisztviselőjének és dolgozójának meg kell ismernie és annak betartásért felelősséggel tartozik.

Kelt: Pomáz, 2012. október 25.

POMÁZ VÁROS JEGYZŐJE

.....

jegyző

1. számú melléklet

A Polgármesteri Hivatal által elektronikus úton, számítógéppel készített dokumentumok biztonságos tárolásához történő hozzáférés és a különböző jogosultsági szintek

Hozzáférési csoportok

1. Adócsoport
2. Alpolgármester
3. Beruházási csoport
4. Építéshatósági csoport
5. Főépítész
6. Gyámhivatal
7. Informatika
8. Jegyző
9. Költségvetési elemző
10. Közbeszerzési jogász
11. Közigazgatási Csoport
12. Közterület Felügyelet
13. Népjóléti csoport
14. Pénzügyi csoport
15. Polgármester
16. Szervezési csoport

A hivatal minden dolgozója ezen csoportok valamelyikébe tartozik. Egy dolgozó több csoport tagja is lehet.

A dolgozók a Hivatal informatikai rendszerében elsősorban az alapján kapnak hozzáférést, hogy mely csoportba tartoznak.

Jogosultságok

A Hivatal dolgozói az általuk számítógéppel készített, vagy kapott anyagokat azok természeténél fogva különböző helyen kell tárolják:

1. Azok a dokumentumok, melyekhez a Hivatal más dolgozóinak egyáltalán nem szabad hozzáférnie: **O meghajtó** (privát hozzáférés)
2. Azok a dokumentumok, melyekhez betekintésre a dolgozó saját csoportjának tagjai is hozzáférhetnek: **X meghajtó** (csoportos hozzáférés)
3. Azok a dokumentumok, melyekhez betekintésre a Hivatal összes dolgozója hozzáférhet: **Y meghajtó** (hivatali szintű hozzáférés)

Az tehát, hogy a dolgozó egy adott dokumentumot hol helyez el (hova ment el) egyértelműen meghatározza, hogy ki és milyen feltételekkel férhet hozzá.

A dolgozó és csoportjának vezetője közösen felelnek azért, hogy a dolgozó által készített dokumentumok a megfelelő helyre legyenek elhelyezve, elmentve. A dokumentumok nem megfelelő helyen történő elhelyezése ugyanis illetéktelen hozzáférést eredményezhet.

A Saját számítógép: a hozzáférések itt nem állíthatók be pontosan. Használata nem, vagy csak alárendelt esetekben javasolt.

2. sz. melléklet

MEGISMERÉSI NYILATKOZAT

Jelen szabályzat tartalmát a mai napon megismertem, az abban foglaltakat munkaköröm ellátása során kötelező érvényűnek tartom.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Kelt: .....

.....

Aláírás