BUDAPEST FŐVÁROS I. KERÜLET BUDAVÁRI POLGÁRMESTERI HIVATAL JEGYZŐJÉNEK 10/2024. (IV. 15.) SZÁMÚ NORMATÍV UTASÍTÁSA A BUDAPEST FŐVÁROS I. KERÜLET BUDAVÁRI POLGÁRMESTERI HIVATAL INFORMATIKAI BIZTONSÁGI SZABÁLYZATÁRÓL

BUDAVÁRI
POLGÁRMESTERI HIVATAL

Budapest 2024.

Dokumentum változáskövetés

Dátum	Verzió	A változás oka	A módosítást elvégezte
2023.06 hó	V1	2013. évi L. Tv. és a 41/2015 BM rendelet miatti kialakítás	Ritek Zrt.
2024 03-04. hó	V2	Egyeztetés a PH-val	Ritek Zrt.

Tartalomjegyzék

I. Bevezetés

Budapest Főváros I. kerület Budavári Polgármesteri Hivatal (továbbiakban Hivatal) *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény* (továbbiakban Ibtv.) valamint a végrehajtására kiadott, *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről* szóló 41/2015. *(VII.15.) BM rendelet* (továbbiakban Vhr.) alapján eljárva megalkotja Budapest Főváros I. kerület Budavári Polgármesteri Hivatal Informatikai Biztonsági Szabályzatát **(továbbiakban: Szabályzat).**

1. A Szabályzat célja, hogy eleget tegyen:

a) az Ibtv. 7. § (3) bekezdésében foglaltaknak: „A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni."

b) az Ibtv. 10. § (8) bekezdésében foglaltaknak: „A szervezet vagy felelős szervezeti egység biztonsági szintbe sorolását a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági szintbe sorolás eredményét a szervezet informatikai biztonsági szabályzatában vagy szervezeti egységre irányadó szabályzatban kell rögzíteni."

c) az Ibtv. 11. § (1) bekezdésében foglaltaknak: „A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről:
   - az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
   - meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,
   - gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
   - rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
   - gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
   - biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
   - ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
   - ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
   - felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,

- megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

II. Fogalmak a jelen Szabályzat alkalmazásában

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

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

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

adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

adattrezor-archiválás: az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési tv.) 25. § (4a) bekezdése szerinti, az elektronikus ügyintézést biztosító szervnek az ügyek intézésével kapcsolatos, elektronikus információs rendszereiben és nyilvántartásaiban tárolt nem minősített adatai biztonsági mentése

adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés;

bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül

biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;

biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

biztonsági szint: a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban

meghatározott biztonsági feladatok kezelésére;

biztonsági szintbe sorolás: a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;

életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;

észlelés: a biztonsági esemény bekövetkezésének felismerése.

fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.

hatóság: a Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet;

kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

korai figyelmeztetés: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb

közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;

Minimális üzletmenet-folytonossági célkitűzés (MBCO): a hivatali szolgáltatásoknak az a minimális szintje, amely az üzletmenet-folytonosság megszakadása esetén elégséges a Hivatal alapfeladatainak és működésének ellátásához;

rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

rendkívüli esemény: minden olyan esemény, amely a Hivatal és intézményei tevékenységének folyamatosságát támogató informatikai rendszerek folyamatos, üzemzavar mentes működőképességét veszélyezteti, vagy akadályozza;

sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

üzemzavar: az az állapot, amikor az informatikai rendszerek működésében rövid idejű zavar keletkezik, s így a rendszer néhány funkciójának átmeneti meghibásodása következik be, a zavar elhárítását az Informatikai Csoport a napi rutinja alapján a BCP életbe léptetésénél rövidebb idő alatt képes elvégezni;

III. A Szabályzat hatályai.

1. Szabályzat személyi hatálya, szerep- és felelősségi körök.

Jelen Szabályzat a személyi hatályok vonatkozásában az alábbiak szerint állapítja meg a célokat, a Szabályzat tárgyi és személyi hatályát, az elektronikus információbiztonsággal kapcsolatos szerepköröket, a szerepkörhöz rendelt tevékenységeket a tevékenységekhez kapcsolódó felelősségeket az információbiztonság szervezetrendszerének belső együttműködését, az emberi tényezőket figyelembe vevő személybiztonsággal kapcsolatos intézkedésekkel érintetteket.

A Szabályzat személyi hatálya kiterjed a

A) Hivatal valamennyi:
- tisztviselőjére,
- köztisztviselőjére, ügykezelőjére, egyéb jogviszonyban álló dolgozójára
- a képviselő-testület tagjaira,
- tisztségviselőjére,

- a hivatali informatikai rendszerekhez hozzáférő bizottsági tagokra,
- a hivatali informatikai rendszerekhez hozzáférő külsős bizottsági tagokra,
- a fő- és másodállású, mellék- és részfoglalkozású munkatársára,
- a hivatalban foglalkoztatott közcélú foglalkoztatottakra,

B) Válságkezelő Csoport (továbbiakban: VKCS), amelynek tagjai:
   - a Jegyző, kockázatgazda: a Hivatal Jegyzője vagy a Jegyző helyettese, aki a VKCS vezetője is egyben,
   - az Informatikai biztonságért felelős személy,
   - a Gazdasági Iroda vezetője,
   - a kommunikációs vezető,
   - a Hivatal szervezeti egységek - Jegyző által kijelölt - egyes vezetői,
   - az Épület-karbantartási vezető: Üzemeltetési és Informatikai Csoport vezetője

C) DRP Kiemelt, Kulcsfelhasználó: a Hivatal foglalkoztatásában álló munkavállaló, aki az üzletmenet folytonosság biztosítása során privilegizált vagy a szokványostól eltérő jogosítványokkal rendelkezik.

D) Ügyfelekre: Azok a természetes személyek, akiknek az Önkormányzat vagy a Hivatal hatáskörébe vagy feladatkörébe tartozó ügyben a Hivatal épületeibe történő belépése ügyintézés céljából szükséges.

E) Vendégekre: Különösen, a látogatók, érdeklődők, rendezvény résztvevői, a sajtó és média képviselői.

F) Külső munkavállalókra: A Szabályzat személyi hatálya kiterjed olyan külső munkavállalóra, aki a munkaköréből, tevékenységéből fakadóan a hivatali hálózatot használja.

G) Szerződő felekre: A Szabályzat személyi hatálya kiterjed olyan külső jogi vagy természetes személyre, akik egyéb jogviszony alapján és titoktartási nyilatkozat tételét követően a hivatali hálózatot használják (különösen rendszerüzemeltetők, Full Service Support szolgáltatást nyújtók).

A Hivatalban ellátott szerepük szerint **a felelős személyeket és a felelősségi köröket,** valamint a munkaköröket, feladatokat az alábbi személyekre vonatkozóan az IBSZ szabályozza:

- Jegyző: a Hivatal Jegyzője
- Kockázatgazda: a Jegyző vagy a helyettese
- Gazdasági Iroda Vezetője
- Informatikai biztonságért felelős személy
- Üzemeltetési és Informatikai Csoportvezető
- Hivatal szervezeti egységek vezetői
- Informatikai üzemeltető, rendszergazda
- Informatikai ügyintéző
- Felhasználó: hivatali dolgozó
- Portaszolgálatot ellátó személy

2. A Szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya kiterjed:

a) valamennyi (a Hivatal tulajdonában lévő, vagy általa bérelt, munkavégzéshez használt) informatikai és telekommunikációs berendezésre, beleértve a berendezések műszaki dokumentációját is;
b) a hivatali eszközökön működtetett rendszerprogramokra és a felhasználói programokra, beleértve a távoli rendszerek használatát is;

c) az informatikai folyamatban szereplő valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentációk);
d) az adathordozók tárolására és felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhoz történő eljuttatás folyamatait is;
e) az adatok felhasználására vonatkozó utasításokra;
f) a védelmet élvező adatok teljes körére, keletkezésük és felhasználásuk, valamint feldolgozásuk helyétől, továbbá a megjelenési formájuktól (bizonylatok, tablók, adathordozók, stb.) függetlenül;
g) hivatali munkavégzéshez jelen Szabályzatban meghatározott feltételekkel engedélyezett saját eszközökre.

3. A Szabályzat területi hatálya

A Szabályzat területi hatálya kiterjed a következő hivatali helyszínekre:

Valamennyi Budapest Főváros I. kerület Budavári Polgármesteri Hivatal tulajdonában vagy használatában álló épületre, ha abban a hivatali hálózatba kapcsolt informatikai, távközlési vagy irodatechnikai rendszer működik.

Így különösen, de nem kizárólag:

a) 1014 Budapest, Kapisztrán tér 1.
b) 1014 Budapest, Úri utca 58.
c) 1013 Budapest, Attila út 65.
d) Egyéb helyszínek. Minden olyan helyszínre, amelyen szerződés szerint a Hivatal információs rendszeréhez hozzáférés történik, beleértve a tartalék helyszínt is. Az ilyen hozzáférések részleteit jelen Szabályzatban meghatározott feltételekkel szerződésben rögzíteni kell, valamint a távoli hozzáférésre vonatkozó védelmi intézkedéseket maradéktalanul el kell végezni.
e) Külső munkavégzés, ellenőrzés. A Hivatal munkavállalói által más helyszínen (például de nem kizárólag: ellenőrzés során vagy otthoni munkavégzés esetén) történő munkavégzésre, amennyiben a munkavégzés a Hivatal informatikai eszközein és/vagy a hálózatára távolról kapcsolódva történik.
f) Külső katasztrófa elhárítási munkavégzési helyszín, amikor a Jegyző utasítására a munkavállalók más helyszínen (például, de nem kizárólag: Budavár önkormányzatának 100%-os tulajdonában levő gazdasági társaságánál és / vagy fenntartásában levő intézményénél végzett üzemeltetés, ellenőrzés során vagy otthoni munkavégzés esetén) történő munkavégzésre kerül sor, amennyiben a munkavégzés a Hivatal informatikai eszközein és/vagy a hálózatára távolról kapcsolódva történik.

IV. A Szabályzat felülvizsgálata

4. Jelen Szabályzatot felül kell vizsgálni:

a) ha a Szabályzat tárgyi, területi vagy személyi hatályában változás történik,
b) ha jogszabály vagy jogszabályváltozás előírja,
c) ha a hivatali szervezetben, biztonsági besorolásban vagy a belső szabályozókban olyan változás történik, amely kihatással van a Szabályzat tartalmára,
d) ha olyan technológia-változás történik, amely azt indokolja,
e) ha a személyi hatályban érintettektől módosítási javaslat érkezik,

5. A Szabályzat frissítése, módosítása

a) Amennyiben a belső és / vagy külső felülvizsgálat indokolja, akkor a Szabályzatot módosítani vagy frissíteni kell.

b) A kockázatelemzést minden olyan esetben meg kell ismételni, amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, különösen: a védendő értékekben változás történik; a fenyegetettségben jelentős változás áll be; jogszabály vagy jogszabályváltozás előírja.

c) Jelen Szabályzat módosításával kapcsolatos javaslattételre jogosult minden érintett, aki jelen Szabályzat személyi hatálya alá tartozik. A javaslattételt írásban, indokolással kiegészítve a szervezeti egység vezetők teszik meg az Üzemeltetési és Informatikai Csoportvezetőnek, aki a javaslattételt megvizsgálja technikai kivitelezhetőségi, költségráfordítási (beleértve a humán erőforrás-ráfordítás tervezett költségét is) szempontból, valamint egyezteti az Információbiztonsági Felelőssel, aki információbiztonsági szempontból vizsgálja meg azt. Az így elfogadott javaslatot döntés-előkészítési javaslat formájában Jegyző elé tárja, aki dönt a Szabályzat módosításáról vagy annak elvetéséről.

d) A frissítéseket, módosításokat dokumentáltan, változáskövetéssel, vagy módosító Szabályzat esetén egységes szerkezetre alakítással kell elvégezni. A dokumentálásnak tartalmaznia kell a módosító személy nevét, a módosítás időpontját, a módosítás okát, a folytonosan növelt verziószámot.

e) A módosítás minden esetben tartalmazza a hatályba lépés időpontját.

6. A Szabályzat megismerése, kihirdetése

1. A Szabályzatot kizárólag azok a személyek ismerhetik meg, akiknek a körét a Jegyző jóváhagyta. Tilos a Szabályzatot publikus felületen közzétenni vagy harmadik személy által hozzáférhetővé tenni.
2. A Szabályzat, a Jegyző aláírásával és bélyegzőlenyomatával hitelesített papír alapú dokumentum képként történő beszkennelése során keletkező Portable Document Format (PDF vagy CPDF) formátumú és a módosítható állományt kizárólag az Üzemeltetési és Informatikai Csoportvezető tárolhatja olyan jogosultsággal, hogy módosítási joga a dokumentumon másnak nem lehet.
3. A Szabályzatot elektronikusan aláírt formában is lehet tárolni a 3. pontban meghatározott módon.
4. A Szabályzat végleges, legutolsó verziójú, módosítható szövegszerkesztő állományát adathordozón az Üzemeltetési és Informatikai Csoport páncélszekrényeiben is tárolni kell.
5. A Szabályzat tartalmának ismertetése – különösen a biztonság tudatos képzés és a feladat alapú biztonsági képzés – a Szabályzat alanyi hatálya alá tartozó természetes és jogi személyek képviselőinek számára, a Jegyző utasítása szerint történik.
6. Új hivatali dolgozó munkába állásakor és / vagy az informatikai rendszer bármely eleméhez történő hozzáférésének feltétele, hogy a dolgozó írásbeli nyilatkozatot tesz jelen Szabályzatban foglaltak megismeréséről, betartásáról, a fegyelmi felelősségekről.
7. A Szabályzat módosításakor minden hivatali és a Szabályzat személyi hatálya alá tartozó felhasználó köteles nyilatkozatot tenni a módosított Szabályzatban foglaltak megismeréséről, betartásáról, a fegyelmi felelősségekről.
8. A Szabályzat módosításakor lehetőség van a nyilatkozatot szervezeti formában aláírni (egy nyilatkozaton a teljes szervezeti egység összes dolgozója egymás alatt felsorolva, folyamatos számozással ellátva olvasható névvel, aláírással és dátummal nyilatkozhat.
9. Az a felhasználó, aki nem nyilatkozik a Szabályzat megismeréséről és betartásáról nem jogosítható fel

a Hivatal információs rendszerének használatára, a meglévő jogosultságokat a nyilatkozat megtételéig azonnali hatállyal meg kell szüntetni.

7. Kapcsolódó jogszabályok, szabályzatok, eljárásrendek, dokumentumok

1. a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló az EU Parlament és Tanács 2016/679. számú Rendelete (GDPR),
2. a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló EU Parlament és a Tanács 910/2014/EU Rendelete,
3. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infó tv.),
4. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény,
5. az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény,
6. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet ,
7. az önkormányzati ASP rendszerről szóló 257/2016 (VIII.31.) Kormány rendelet,
8. az elektronikus ügyintézés részletszabályairól szóló 451/2016 (XII.19.) Kormány rendelet,
9. a Kormányzati Adatközpont működéséről szóló 467/2017. (XII. 28.) Korm. rendelet,

10. Budapest Főváros I. kerület Budavári Polgármesteri Hivatal:

    a) Üzletmenet-folytonossági Terv, Szabályzata (BCP),
    b) Adatvédelmi Szabályzata,
    c) Informatikai Okirati Minták
    d) Külsős vállalkozók és hatóságok Jegyzéke,
    e) Információátadási Szabályzata,
    f) Tűz- és munkavédelmi Szabályzata,
    g) Adatkezelési és adatvédelmi Szabályzata,
    h) Infrastruktúra terve,
    i) Beszerzési Szabályzata,
    j) Képzési terve,
    k) Kockázatkezelési Szabályzata;

V. Felelősségi körök és feladatok.

A szerepkörökhöz kapcsolódó felelősségi körök a következők.

8. A Jegyző, kockázatgazda:

a) az Ibtv. 7. § (3) bekezdése alapján a Hivatal biztonsági osztályba sorolását a Jegyző hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért;
b) Jegyző felel a biztonsági osztályba sorolás jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért; a biztonsági osztályba sorolást a szervezet

informatikai biztonsági Szabályzatában kell rögzíteni;

c) kockázatgazdaként biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
d) kockázatgazdaként biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
e) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
f) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági Szabályzatot,
g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
j) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
k) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
l) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
m) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket,
o) jogosult a biztonsági esemény bekövetkezésének kihirdetésére;
p) jogosult elrendelni - az üzletmenet-folytonosság biztosítása érdekében - a tartalék feldolgozási helyszín és az ott telepített eszközök használatba vételét, a szervezeti feladatok területi ellátásának átszervezését (diszlokálás);
q) kijelöli a Hivatal szervezeti **egységek egyes vezetőit,** akik a katasztrófa elhárítás megszervezésében az általa megbízott feladatokkal rendelkeznek, a probléma megoldásokra vonatkozó javaslat megtételére alkalmasak lehetnek, az üzletmenet folytonosság biztosításában kiemelt szervező feladatuk lehet;
r) jogosult a biztonsági esemény megszűnés kihirdetésére.

9. Az Informatikai biztonságért felelős személy.

a) A Hivatal vezetője által az Ibtv. 11. § (1) c) pont felhatalmazása alapján kinevezett elektronikus információs rendszer biztonságáért felelős személy.
b) A Hivatalban csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel. Nem kell az előzőek szerinti képzettséget megszereznie, ha rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.
c) A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést

igazolja.

d) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését. Az elektronikus információs rendszer biztonságáért felelős személy Ibtv. szerinti feladatai és felelőssége ez esetekben más személyre nem átruházható.
e) Az elektronikus információs rendszer biztonságáért felelős személy jogosult az e bekezdés szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.
f) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.
g) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért.
h) Gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.
i) Elvégzi vagy irányítja az előző pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.
j) Előkészíti a szervezet elektronikus információs rendszereire vonatkozó Informatikai Biztonsági Szabályzatot.
k) Előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását.
l) Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő Szabályzatait és szerződéseit.
m) Kapcsolatot tart a Nemzeti Kibervédelmi Intézettel.
n) Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.
o) Katasztrófa helyzetben utasítja: a Hivatal Vezetője.
p) Katasztrófa helyzetben beszámol: a Hivatal Vezetőjének és köteles együttműködni a hatósággal.
q) Felelősségi köre katasztrófa helyzetben kiterjed:
    - A katasztrófa helyzetre történő felkészülésért;
    - A katasztrófa gyanús rendkívüli események elemzésére;
    - Korai figyelmeztetés kiadására;
    - Valamennyi érintett értesítésére a katasztrófa helyzetről és a közreműködés elvárt módjáról;
    - A katasztrófa elhárításhoz kapcsolódó valamennyi tevékenység megszervezésére és menedzsmentjére;
    - A tartalék feldolgozási helyszínen a védett zónák meghatározására, a meglevők módosítására, a beléptetési rendszer meghatározására;
    - A katasztrófa helyzettel kapcsolatos döntési javaslatra;
    - A felügyeleti hatóság katasztrófa jellegétől függő tájékoztatására a katasztrófa helyzetről;
    - A tartalék eszközökre történő átállásra;
    - A katasztrófa helyzet alatti tevékenységek dokumentálásának megszervezésére;
    - A katasztrófa helyzet elleni védelmet szolgáló oktatására és tesztelésre.

10. Üzemeltetési és Informatikai Csoportvezető feladatai és felelőssége.

A) Az informatikai feladatokra vonatkozóan:

a) Ellátja az Informatikai vezetői feladatokat, meghatározza a munkatársak feladatait, ellenőrzi a feladatok elvégzését, értékeli a munkavégzést, engedélyezi a csoporthoz tartozó rendes szabadságolást.
b) Kidolgozza és kidolgoztatja, és folyamatosan aktualizálja a város informatikai (és a kapcsolódó

telekommunikációs) koncepcióját, stratégiáját, összhangban a Hivatal informatikai biztonsági politikájával, stratégiájával.

c) Koordinálja az Informatikai fejlesztési beruházásokat. Ellenőrzi a teljesítéseket.
d) Irányítja a Hivatal informatikai rendszer biztonságos környezetének kialakítását, a rendszer működtetésének és felügyeletének munkálatait.
e) Irányítja a változásfelügyeletet (change control), felügyeli az eljárásokat, amelyek biztosítják, hogy minden változás ellenőrzött legyen, beleértve annak kérelmezését, rögzítését, elemzését, a vonatkozó döntés meghozását, jóváhagyását, tesztelését, üzembe állítását és a változás megvalósítás utáni áttekintését is.
f) Irányítja a Hivatalban fellelhető adatok, egységes adatbázisba szerkesztését, s koordinálja ezek feltöltését, a meglévő adatokból.
g) Kidolgozza és kidolgoztatja a Polgármesteri Hivatal informatikai Szabályzatait, koordinálja annak betartására irányuló munkát.
h) Részt vesz a Hivatal hardware és software beszerzéseinek előkészítésében.
i) Folyamatos kapcsolatot tart az Informatikai dolgozókkal, segíti munkájukat.
j) Biztosítja a Hivatal telefonhálózatának működtetését.
k) A köztisztviselőként felelős a szervezeti egységben dolgozók munkájának koordinálásáért.
l) Felelős továbbá az osztály dolgozói által elvégzett munkák ellenőrzéséért
m) Felelős az informatikai Szabályzatok aktualizálásáért, betartásáért, betartatásáért
n) A munkájával összefüggő vagy rábízott beszerzések szakmai anyagának teljeskörűségéért, a leszállított termékek ellenőrzéséért, tételes átvételéért
o) Felelős továbbá az általa elvégzett adatszolgáltatás és adminisztráció pontosságáért, naprakészségéért, teljeskörűségéért

B) Az épület-üzemeltetési feladatokra vonatkozóan

a) Feladatai és felelőssége:
   - A víz- és más, csővezetéken szállított anyagok csővezeték-hálózatának nyomvonala, valamint a főelzáró csapok és szelepek működésének biztosítása, valamint helyének ismertetése az informatikai személyzettel, illetve a katasztrófa-elhárításban részt vevő személyekkel.
   - Szükség esetén – amennyiben az veszélyeztetheti az informatikai rendszerek működését – biztosítja a csővezetékek áthelyezését.
   - Az erősáramú elektromos hálózat nyomvonalának és főkapcsolóinak ismertetése az informatikai személyzettel, valamint a katasztrófa-elhárításban részt vevő személyekkel.
   - Szükség esetén részt vesz az informatikai rendszereket vagy azok biztonságát szolgáló épületi, épületgépészeti vagy villamossági kialakításokban.
   - Részt vesz az elemi és környezeti károk megelőzésével kapcsolatos feladatokban, valamint a bekövetkezett károk javításában.

b) Katasztrófa helyzetben utasítja: a Jegyző
c) Katasztrófa helyzetben beszámol: a Hivatal vezetőjének
d) Felelősségi köre Katasztrófa helyzetben kiterjed:
   - A tartalék helyszín felkészítéséért, szinten tartásáért a katasztrófahelyzet szerinti működésre;
   - Az alternatív és normál munkavégzéshez szükséges helyszínek és azok berendezésének, valamint az irodaszerek biztosítása a legjobb szaktudása szerint;
   - A helyszínek kialakításáról a Jegyző és az Informatikai biztonságért felelős személynek történő folyamatos és naprakész tájékoztatása;
   - A DRP Kiemelt felhasználók szükség szerinti átszállítására DRP gyakorlat és vészhelyzet esetén;
   - A bútorok, informatikai továbbá egyéb szükséges eszközök átszállításáért a tartalék helyszínre;

11. A Hivatal szervezeti egységek vezetői: a Hivatal Szervezeti és Működési Szabályzatában meghatározott szervezeti egység vezetői (irodavezetők, csoportvezetők)

a) Feladataik és felelősségük:
   - Jelen Szabályzatban előírtak helyi betartásának megkövetelése és a betartás ellenőrzése.
   - Jelen Szabályzatban meghatározott felhasználói azonosítás-hitelesítési és fiókkezelési eljárás során kezdeményezi a szervezeti egységébe tartozó munkavállalók szervezeti egységhez kapcsolt jogainak beállítását, módosítását, illetve megszüntetését.
   - Jelen Szabályzatban meghatározott időközönként a jogosítás-ellenőrzési pontban meghatározottak szerint ellenőrzi a szervezeti egységébe tartozó munkatársak jogosultságának megfelelőségét, a hivatali apparátusból távozott beosztottjai jogainak visszavonását.
   - A közvetlen feletteséнél kezdeményezi az alkalmazás-katalógustól eltérő vagy a szervezeti egységében nem engedélyezett alkalmazás-telepítési, a szervezeti egységén túlmutató jogosítási és/vagy adatkapcsolati feladatok, valamint külső adatbázisokhoz történő kapcsolódás engedélyezését.

b) Katasztrófa helyzetben utasítja: a Jegyző
c) Katasztrófa helyzetben beszámolnak: a Hivatal vezetőjének
d) Felelősségi körük Katasztrófa helyzetben kiterjed:
   - A Kiemelt DRP felhasználók személyi körének meghatározására;
   - A Kiemelt DRP felhasználók utasítására a tartalék feldolgozási helyszín elérése érdekében;
   - Az alárendelt és az eredeti telephelyen maradó felhasználók vészhelyzet alatti munkautasításokkal való ellátására;
   - A portaszolgálatot ellátó személyek tartalék feldolgozási helyszínen történő feladat ellátására;
   - A tartalék helyszín munkaállomásainak munkafelvételének megszervezésére;
   - A Kiemelt DRP felhasználók munkájának megszervezésére a tartalék helyszín munkaállomásainak elfoglalása után;
   - A lehetséges hivatali ügyfelek tájékoztatására;
   - Döntési javaslatok megtételére az üzletmenet-folytonosság biztosítására vonatkozóan;
   - Minden munkaintézkedés megtételére az alapszintű szolgáltatás újra elérésére

12. A Pénzügyi vezető: a Gazdasági Iroda vezetője.

a) Feladatai és felelőssége:
   - pénzügyi erőforrások biztosítása;
   - költségvetés tervezés, és a beruházások, beszerzések során tervezi az informatikai biztonsági stratégia megvalósításához szükséges forrásokat, dokumentálja e követelmény alá eső kivételeket;
   - intézkedik a terveknek megfelelő kiadásokhoz szükséges erőforrások rendelkezésre állásának biztosítása iránt;
   - gondoskodik a Hivatal informatikai eszközeinek és alkalmazásainak leltárának napra készen tartásáról az informatikusok által kitöltött és átadott bizonylatok, átadás-átvételi jegyzőkönyvek, selejtezési jegyzőkönyvek alapján;
   - gondoskodik a beszerzett eszközök és alkalmazások állományba vételéről;
   - gondoskodik a Hivatalban alkalmazott a Hivatal folyamataira – kivéve az informatikai kockázatkezelési folyamatokat – vonatkozó kockázatkezelési és -elemzési Szabályzat napra készen tartásáról;
   - haladéktalanul tájékoztatja az Informatikai Csoport vezetőjét, amennyiben új hivatali kockázat merül fel és/vagy a kockázatkezelési Szabályzatban változás történik.

b) Katasztrófa helyzetben utasítja: a Jegyző
c) Katasztrófa helyzetben beszámol: a Hivatal vezetőjének.
d) Felelősségi köre Katasztrófa helyzetben kiterjed:

- A költségvetés tervezésre, és a beruházások, beszerzések során tervezi az informatikai biztonsági stratégia megvalósításához szükséges forrásokat, dokumentálja e követelmény alá eső kivételeket;
- Intézkedik a terveknek megfelelő kiadásokhoz szükséges erőforrások rendelkezésre állásának biztosítása iránt;
- Gondoskodik a beszerzett eszközök és alkalmazások állományba vételéről;
- A tartalék helyszín munkaállomásainak munkavégzés céljából való berendezésére;
- A tartalék eszközökre történő átállásra; a Hivatal pénzügyi szolgáltatásainak redundáns biztosítására;
- A banki szolgáltatások tartalék helyszínről vagy a pénzintézetnél történő elérés biztosítására;
- A hivatali ügyfelek számára a tartalék helyszínen a házipénztári és a készpénzkímélő, továbbá a bankkártyás szolgáltatások biztosítására;
- A Hivatal vezetője által priorizált üzletmenet-folytonosságot biztosító munkafeladat elvégzésére, a minimális szolgáltatás biztosítására;
- Készpénz állomány biztosítása a tartalék infrastruktúra pótlása és vagy az üzletmenet-folytonosság biztosítása céljából szükséges rendkívüli beszerzések érdekében;
- Tevékenységének alapvető dokumentálására.

13. Informatikai üzemeltetők, rendszergazdák

a) Feladataik és felelősségük:

- Részt vesznek a Polgármesteri Hivatal informatikai rendszerének üzemeltetésében, karbantartásában különös tekintettel a munkaköri leírásában szereplő szervezeti egységeket érintő kliens- és szerveroldali rendszerek vonatkozásában.
- Az általuk üzemeltetett rendszerek vonatkozásában szerver és kliens oldali szoftvereket telepítenek a jogszabályi és licence előírások figyelembe vételével.
- Az üzemeltetett rendszerek felhasználói, kliens változásait, a hardver és egyéb elemeit nyilván kell tartaniuk, továbbá a változásoknak megfelelően módosítaniuk kell a Hivatal informatikai leltár rendszerben.
- A licenceket a nyilvántartásban pontosan, visszakereshetően adminisztrálják. Folyamatosan figyelemmel kíséri a használt rendszerek javítócsomagjainak frissülését, telepíti a javítócsomagokat.
- Az üzemeltetett rendszerek vonatkozásában informatikai, távközlési és irodatechnikai eszközöket telepítenek, javítanak, javíttatnak, szükség esetén cserélnek.
- Gondoskodnak a megfelelő számú alkatrész raktáron tartásáról, a közbeszerzési eljárás időtartamának figyelembe vételével időben jelzik, ha a raktárkészletben bármelyik alkatrész olyan mértékű fogyását tapasztalja, amely az alkatrészellátás folyamatosságát veszélyezteti. Az alkatrészeket és helyüket pontosan, visszakövethetően adminisztrálják a nyilvántartásban. Az eszközök mozgását az előírások szerint dokumentálják.
- Az Informatikai biztonságért felelős személy kérésének megfelelően meghatározott időpontokban részletes kimutatást készítenek a Hivatalban üzemeltetett elektronikus információs rendszer elemeiről, különösen a kliens számítógépekről, a multifunkcionális eszközökről, az IP számokról, a hálózati végpontokról, kiemelt fontosságú szoftverek jogosultjairól, a nyomtatókról.
- Felelősek továbbá az általuk elvégzett adatszolgáltatás és adminisztráció pontosságáért, naprakészségéért, teljeskörűségéért.
- Az üzemeltetett rendszerek vonatkozásában folyamatosan figyelemmel kísérik az adatbiztonságot.

- Gondoskodnak a vírus- és betörésvédelemről, a hálózati elemeket, szervereket és kiemelt felhasználói (superuser) számítógépeket tartalmazó helyiségek fizikai adathozzáférés elleni védelméről. Különös figyelmet fordítanak arra, hogy ezen helyiségekbe kizárólag – naplózottan -- a belépési jogosultsággal rendelkezők juthassanak be.
- Az üzemeltetett rendszerekkel összefüggésben elvégzik a szakirodai jogosításokat, a szakiroda vezetőjének javaslata szerint. A módosításokat folyamatosan naplózzák. Felelősek a jogosításokért, azok biztonságáért, a jogosítási mátrix vezetéséért, biztonságos tárolásáért. Az iroda hatáskörén túlmutató igényeket jegyzői engedéllyel módosítják.
- Gondoskodnak az általuk üzemeltetett rendszerek vonatkozásában a napi inkrementális és heti teljes mentésről, az adatok éves és a rendszerállományok módosításkori archiválásáról. A biztonsági mentések visszaállíthatóságát havonta, az archívokat az elkészítésüket követően ellenőrzik. Az archívok visszaállításhoz szükséges rendszereket is archiválják.
- A szerver üzemeltetők gondoskodnak az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendeletben meghatározott és rendszeres adattrezor-archiválás végrehajtásáról.
- Folyamatosan tájékozódnak az általa üzemeltetett rendszerek vonatkozásában a felhasználói igényekről, a megjelenő új szoftvertermékekről, védelmi eszközökről indokolt esetben javaslatot tesznek a bevezetésükre.
- Megfelelő szigetalkalmazásokat telepítenek, gondoznak. Javítás, verziófrissítés, telepítés esetén együttműködnek a felhasználókkal, a fejlesztőkkel.
- Felettesei utasítása szerint részt vesznek az informatikai adat- és információszolgáltatásban, adatkommunikációban.
- A beszerzett eszközöket rögzítik a nyilvántartásban, zárt raktáron tartják, a raktárkészletet kezelik, átvetetik, visszaveszik, bizonylatolják. A munkájával összefüggő vagy rábízott beszerzések szakmai anyagának teljeskörűségéért, a leszállított termékek ellenőrzéséért, tételes átvételéért felelősek.
- Az általuk használt vagy kiadott eszközök és szoftver-license-k bizonylatolásáért, valamint a nyilvántartóban történő pontos, naprakész vezetéséért anyagi felelősséggel tartoznak.
- A kritikus eszközökből tartalékot képeznek, folyamatosan tájékoztatják a felettest az eszközkészletről. Működés szempontjából kritikus rendszerelemekből tartalékképzésért, a tartalék felhasználásakor a rossz eszköz javításáért vagy új eszköz időben történő beszerzéséért felelősek.
- Kapcsolatot tartanak a szolgáltatókkal, hibabejelentést végeznek, javítást koordinálnak.
- A telefonközpont használatához szükséges biztonsági kódokat kezelik, kiadják, visszaveszik, nyilvántartást vezetnek, a megfelelő hozzáférés- és adatvédelem, valamint a mindenkori adatarchiválás biztosításával. Gondoskodnak a visszavett kódok működésképtelenségének beállításáról. A Jegyző utasításai alapján lekérdezéseket, statisztikákat készítenek a telefonálási szokásokról.
- Folyamatosan figyelemmel kísérik a jogszabályokat és a belső Szabályzatokat, különösen a közigazgatási és az informatikai vonatkozásúakat, betartja, betartatják azokat. Indokolt esetben javaslatot tesz a belső Szabályzatok módosítására, karbantartására. Jogszabály vagy belső Szabályzat megsértésének vagy arra irányuló kísérlet felismerése esetén haladéktalanul megszüntetik azt vagy kísérletet tesznek a cselekmény megszüntetésére, ezzel egyidejűleg értesítik felettesét a cselekményről, annak következményeiről.
- A fent említett rendszerek vonatkozásában az adatmentésért és adatarchiválásért, az adat-visszaállításért, a mentési napló folyamatos vezetéséért, az adatok tárolásáért, azok biztonságáért, a rendszer- és adatfrissítésekért, a naprakész vírusvédelemért.

b) Katasztrófa helyzetben utasítja: a Jegyző és az Üzemeltetési és Informatikai Csoportvezető
c) Katasztrófa helyzetben beszámol: az Üzemeltetési és Informatikai Csoportvezetőnek

d) Felelősségi köre Katasztrófa helyzetben kiterjed:
   - A tartalék helyszín munkaállomásainak munkavégzés céljából való informatikai berendezésére, az

eszközök szállítására, beállítására;
- A tartalék helyszínen a végpontok hálózatba való bekötésére;
- A Kiemelt DRP felhasználók felhasználói profiljának a külön-külön történő beállítására;
- A Kiemelt DRP felhasználókkal történő aktív együttműködésre, ennek keretében a tartalék kliens számítógépek használatára vonatkozó segítségnyújtásra;

14. Kiemelt DRP felhasználók

a) Katasztrófa helyzetben utasítja: a Jegyző, a Hivatal szervezeti egységeinek - Jegyző által kijelölt - egyes vezetői
b) Katasztrófa helyzetben beszámol: a Hivatal vezetőjének és Hivatal szervezeti egységeinek - Jegyző által kijelölt - egyes vezetőinek.
c) Felelősségi köre kiterjed:
   - A tartalék helyszín munkaállomásainak munkafelvételének megszervezésére;
   - A tartalék helyszín munkaállomásainak felhasználói ellenőrzésére, tesztelésére;
   - A lehetséges hivatali ügyfelek tájékoztatására;
   - Döntési javaslatok megtételére az üzletmenet-folytonosság biztosítására vonatkozóan;
   - Minden munkaintézkedés megtételére az alapszintű szolgáltatás újra elérésére

15. Portaszolgálatot ellátó személyek

a) Feladatai és felelőssége:

   - A Hivatal erre jogosult vezetője által meghatározott ellenőrzési ponton, azonosítja és belépteti az arra jogosult személyeket.
   - Megakadályozza, hogy a belépésre nem jogosultak bejussanak, vagy illetéktelenül hozzáférhessenek adatokhoz, információkhoz.
   - Figyeli az illetéktelen behatolási kísérleteket, megakadályozza vagy megakadályoztatja a behatolást.
   - Figyeli és jelzi azokat az elemi környezeti eseményeket, amelyek jelentősen befolyásolják vagy veszélyeztethetik az üzletmenet folytonosságát vagy az adatok bizalmasságát, sértetlenségét, rendelkezésre állásukat.
   - Részt vesz a bekövetkezett károk enyhítésében, szükség esetén az elektromos rendszer vészkikapcsolásával segíti a katasztrófa-elhárítás munkáját.

b) Katasztrófa helyzetben utasítja: a Jegyző, a Hivatal szervezeti egységeinek - Jegyző által kijelölt - egyes vezetői
c) Katasztrófa helyzetben beszámol: a Hivatal vezetőjének és Hivatal szervezeti egységeinek - Jegyző által kijelölt - egyes vezetőinek.

d) Felelősségi köre kiterjed:

   - a katasztrófával érintett épület(ek)ben tartózkodó személyek megfelelő létszámú elhagyásának megszervezésére,
   - a katasztrófával érintett épületben engedéllyel maradó munkavállalók tájékoztatására,
   - a hivatali épületek őrzését, adott esetben lezárására,
   - a tartalék helyszínen az erre jogosultak (VKCS tagjai, a DRP Kiemelt felhasználók) ellenőrzött beléptetésére,

- a hivatali épületbe bejutni kívánó ügyfelek megfelelő tájékoztatására, különösen a tartalék helyszín megközelíthetőségére és az ismert minimális szolgáltatások körére.

16. Felhasználó.

A Hivatal foglalkoztatásában álló munkavállaló, aki egy adott elektronikus információs rendszerben jogosítványokkal rendelkezik, aki a rendszert igénybe veszi.

VI. A hivatali szervezet információbiztonsági belső együttműködése.

a) A Hivatal önálló Üzletmenet-folytonossági Tervvel rendelkezik, amelynek része, de önálló dokumentumként szerepel az Informatikai Katasztrófa-elhárítási Terv.

b) Az Üzletmenet-folytonossági Terv, Szabályzat célja Budapest Főváros I. kerület Budavári Polgármesteri Hivatal által ellátott, kötelező, vagy önként vállalt önkormányzati, jegyző hatáskörébe utalt államigazgatási, valamint egyéb jogszabályokban meghatározott feladatok, ágazati jogszabályokban meghatározott kritikus időn belül történő ellátása, nem várt események vagy cselekmények esetén, helyettesítő eljárások alkalmazásával, az eredeti funkcionalitás helyreállításáig, a kritikus idők, a felelős személyek, tárgyak, eszközök, folyamatleírások biztosításával.

c) A Hivatal különálló Üzletmenet-folytonossági Terv, Szabályzatban megfogalmazza, és a részletezett követelmények szerint dokumentálja, valamint a Hivatalon belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet.

d) Az Üzletmenet-folytonossági Terv, Szabályzat meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket, a kapcsolódó Katasztrófa-elhárítási Szabályzattal (DRP Terv, Szabályzat) összefüggésben rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről, valamint definiálja a szervezet által előzetesen meghatározott alapszolgáltatások fenntartásának menetét, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is.

e) Az információbiztonságot vagy az üzletmenet-folytonosságot érintő, veszélyeztető incidensek vagy megelőző intézkedések szükségessége esetén a Szabályzat hatálya alá tartozó személyek a kötelesek a hatékony együttműködésre.

f) Az együttműködést bármely érintett felelősségi szerepkörben vezető személy kezdeményezheti a Jegyzőnél.

g) A Jegyző jogosult az együttműködésben érintett személyeket egyedi feladattal ellátni, valamint egyeztető megbeszélést összehívni.

h) A Hivatal a szervezeti felépítésének változása esetén, új munkakörök kialakításakor, meglévő munkakörök megszüntetésekor, megváltoztatásakor, összevonásakor, ezek hiányában jelen Szabályzat felülvizsgálatakor felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

VII. A Hivatal elektronikus információs rendszereinek meghatározott biztonsági osztályba sorolása.

1. A Jegyző az Ibtv. 7. § (1) rendelkezése és a Vhr. mellékletének 3.1.2.2. pontja alapján, a Hivatal elektronikus információs rendszereit, az azokban kezelt adatok kockázatokkal arányos védelme biztosítása érdekében, az alábbi biztonsági osztályba sorolja a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából:

bizalmasság szempontjából	4
sértetlenség szempontjából	3
rendelkezésre állás szempontjából	3

2. Ha a Hivatal az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, akkor a vizsgálatot követő 90 napon belül **cselekvési tervet** készít a hiányosság megszüntetésére.

3. Az alkalmazott biztonsági osztály meghatározásával kapcsolatos további feladatok.

   a) Az elektronikus információs rendszer bizalmasság, sértetlenség és rendelkezésre állás szerinti biztonsági osztálya alapján kell megvalósítani az előírt védelmi intézkedéseket az adott elektronikus információs rendszerre vonatkozóan.

   b) Felülvizsgálat. A Hivatal vezetője vagy az általa kijelölt személy a biztonsági osztályba sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén szükséges elvégezni. A soron kívüli felülvizsgálatot akkor is el kell végezni, ha a szervezet státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában változás következik be. Legalább 3 évente a vizsgálatot akkor is meg kell tenni, ha a fenti események egyike sem történt meg.

VIII. A Hivatal által kezelt személyes adatok kezelésének a biztonsági szintbe sorolása.

A Jegyző a GDPR 32. Cikk (2) bekezdésében nevesített biztonság **megfelelő szintjét** a **személyes adatkezeléssel kapcsolatban 3-as értékben határozza meg** az elektronikus információs rendszer elemek - a Közvetlen anyagi kár kockázata, Társadalmi – politikai hatás kockázata, Bizalmasság kockázata, Sértetlenség kockázata, Rendelkezésre állás kockázata - elemzései alapján.

IX. A Hivatal egyes szervezeti egységeinek a biztonsági szintbe sorolása

1. A Jegyző jelen Szabályzat aláírásával az Ibtv. 9. § (2) b) bekezdése és a Vhr. 2. számú melléklet 4. pontjában foglalt meghatározása szerint, a Hivatalban folytatott informatikai üzemeltetési feladatok ellátása miatt, a Hivatal

   - **a fő feldolgozási helyszín**: 1014 Budapest, Kapisztrán tér 1.
   - **a tartalék feldolgozási helyszín:** 1014 Budapest, Úri utca 58.

   ingatlanai és ingatlanrészei esetében mindhárom – bizalmasság, sértetlenség, rendelkezésre állás – összesítésben a **3-as biztonsági szintre** sorolja be, azzal a kikötéssel, hogy az **Informatikusok kezelésében lévő helyiségek besorolása 4-es szintű**.

2. A biztonsági szintbe sorolás a kockázatkezelés keretében végrehajtandó kármegelőzés eszközének minősül az alábbi tények miatt:

A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a Hivatal Üzemeltetési és Informatikai Csoportját az elektronikus információs rendszerek védelmére való felkészültsége alapján biztonsági szintbe kell sorolni a jogszabályban meghatározott szempontok szerint.

X. Adminisztratív védelmi intézkedések

1. Az adminisztratív védelem fogalma.

A védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedéseket, továbbá védelemre vonatkozó oktatást kell érteni.

2. Elektronikus információs rendszerek nyilvántartása.

a) A Hivatal középvezetői a felhasználók munkaköri leírásában szerepeltetik azokat a feladatokat, amelyek az elektronikus információs rendszerek használatát indokolják.

b) A Hivatal az elektronikus információs rendszereiről nyilvántartást vezet; azt összevontan szerepelteti az adatvagyon leltárban, és azt folyamatosan aktualizálja.

c) Az Informatikai üzemeltetők kiterjesztik a nyilvántartást minden rendszerre, a nyilvántartása tartalmazza a rendszerek alapfeladatait; a rendszerek által biztosítandó szolgáltatásokat; az érintett rendszerekhez tartozó licenc számot (ha azok az érintett szervezet kezelésében vannak); a rendszer felett üzemeltetést és / vagy felügyeletet gyakorló személy elérhetőségi adatait; a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek elérhetőségi adatait.

d) Az Üzemeltetési és Informatikai Csoportvezető látja el az adminisztratív védelmi intézkedéseinek a megszervezését, az Információbiztonsági felelőssel egyeztetve.

e) Az elektronikus információs rendszer helyreállításának és újraindításának a végrehajtását az önálló Infrastruktúra terv tartalmazzák.

f) Az elektronikus információs rendszer kapcsolódásait, védelmét az Informatikai biztonsági felelős személy úgy is biztosítja, hogy a Hivatal vezetőjénél kezdeményezi az alkalmazás-katalógustól eltérő vagy a szervezeti egységében nem engedélyezett alkalmazás-telepítési, a szervezeti egységén túlmutató jogosítási és/vagy adatkapcsolati feladatok, valamint külső adatbázisokhoz történő kapcsolódás engedélyezését.

3. Az elektronikus információ biztonsággal kapcsolatos engedélyezési eljárás.

a) Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárásrend a Hivatalban kiterjed minden, az érintett szervezet hatókörébe tartozó az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás eljárási és védelmi követelményszintre és folyamatra, az emberi, fizikai és logikai

erőforrásra.

b) A Hivatal elektronikus információs rendszerein, rendszerelemein történő vagy azokat érintő, azokra kihatással lévő beavatkozásokat megelőzően, minden esetben az alábbi engedélyeztetési eljárásrend szerint kell eljárni.

c) Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó emberi, fizikai és logikai erőforrásra, valamint minden eljárási és védelmi szintre és folyamatra.

d) **Felelősségi körök szétválasztása a** Hivatalban a munkakörök és felelősségi körök dokumentáltan – a munkaköri leírások alapján – szétválasztása kerülnek, ami meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

e) **A Hivatal elektronikus információs rendszereihez történő jogosítás** csak úgy adható ki, ha a felhasználó a Felhasználói Szabályzatot megismerte és a benne foglalt felelősségek tudomásul vételéről írásban nyilatkozik.

f) **Egyedi azonosítás, jogok érdekében a** Hivatal biztosítja, hogy minden munkatársa megfelelő, egyedi és azonosítható hozzáféréssel rendelkezzen a munkaköréhez szükséges a munkaköri leírásában szereplő feladatok ellátásához kapcsolódó informatikai alapszolgáltatásokhoz és személyes vagy csoportos felhasználói fiókjához.

g) **A Hivatal minden munkatársa** számára biztosítja a munkakör ellátásához szükséges felhasználói alkalmazások, illetve a felhasználói alkalmazások meghatározott részeinek rendeltetésszerű használatát megfelelő azonosítási és hitelesítési eljárást követően.

h) **Munkakörhöz kapcsolódó jogok. A Hivatalban** az elektronikus információs rendszerekhez és fiókokhoz kiosztott jogosultságok munkaköri besoroláson alapulnak, ugyanabban a munkakörben dolgozó munkatársak ugyanolyan jogosultságokkal rendelkeznek. Ettől eltérni csak egyedi esetekben, az adott szakiroda vezetője és az Üzemeltetési és Informatikai Csoportvezető engedélyével, dokumentáltan lehetséges.

i) **Hivatali irodai igény** esetén az adott szakiroda vezetője részletes dokumentáció benyújtásával (amely tartalmazza az érintett adatokat, jogosultságokat, adatkapcsolatokat) jelzi a programfejlesztési vagy módosítási, illetve a hibajavítási igényét az Üzemeltetési és Informatikai Csoportvezető felé. Az igényeket minden év elején január 31. napig kell bejelenteni, évközbeni igény vagy jogszabályváltozás esetén a módosítás hatálybalépését megelőzően legalább 90 nappal, de legkésőbb a jogszabály megjelenésekor.

j) **Új dolgozó számára történő infrastruktúra** és jogosultság biztosítása érdekében legalább a munkába állást megelőző 5 munkanappal, a jelenlegi struktúrában történő változás (költözés, igénylés, jogosultság visszavonása) esetén a változást megelőző legalább 3 munkanappal korábban írásban jelezni kell az igényeket.

k) Minden új munkatárs a személyazonosítását követően a Személyzeti dolgozók által kiállított igazolás, valamint a szakiroda vezetőjének írásbeli kérése, illetve a munkavállaló munkaköri leírásában szereplő feladatok alapján a munkaköréhez szükséges adatokhoz, alkalmazásokhoz hozzáférést kap. A szakiroda illetékességén túlmutató jogosultságok kizárólag a szervezeti egység vezetőjének kérésére a mindenkori Jegyző jóváhagyásával állítható be.

l) Külső rendszerek jogosítása a szerződésben meghatározott kapcsolattartókon és azonosítási folyamaton keresztül adható.

m) Az azonosítók kiadásakor ellenőrizni kell, hogy a kiadni kívánt azonosító korábban kiadásra került-e a rendszerben. Nem adható ki olyan azonosító, amely korábban már más személyt azonosított az adott elektronikus információs rendszerben.

n) Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

o) A Hivatalban alkalmazott elektronikus információs rendszerek között létesítendő **belső rendszer kapcsolatokat** az összekapcsolást megelőzően a kockázatelemzési és kezelési tervben szereplő eljárásrend szerint fel kell mérni. Amennyiben az összekapcsolás arányos védelmi intézkedések alapján elvégezhető és az elektronikus információs rendszerek biztonsági osztályba sorolását nem befolyásolja, Jegyző engedélyével végezhető.

4. Az engedélyeztetés folyamata

a) A beavatkozást kérelmező személy megvizsgálja, hogy a biztonságot mérséklő megoldás helyett létezik-e biztonságos módszer a cél elérése érdekében.

b) Amennyiben nem talál ilyet, a szervezeti egysége vezetőjéhez fordul, aki írásban felkéri az Informatikust, hogy vizsgálja meg az adott beavatkozás kockázatát.

c) Az Informatikus a kéréseket visszakereshetően tárolja, egyidejűleg megvizsgálja, hogy a kérés milyen biztonsági kockázatokat rejt, - egyezteti az Információbiztonsági Felelőssel - a cél megvalósítható-e kevésbé kockázatos megoldással, az esetleges védelmi intézkedések arányosak-e a feladattal, valamint költségbecslést és ütemezési tervet készít a védelmi megoldások elvégezhetőségére. A becsléseket javaslattal együtt visszajuttatja a kezdeményező szervezeti egység vezetőjéhez.

d) A kezdeményező szervezeti egység vezetője a kockázatokat, a javaslatot és a becsléseket mérlegeli. Amennyiben a megoldások arányosak a feladatellátás mértékével, forrásmeghatározás mellett feljegyzést készít a Hivatal vezetője számára, aki az Információbiztonsági Felelős javaslata figyelembe vételével dönt a védelmi intézkedések megtételéről és a feladat végrehajtásáról.

e) Az engedélyezett változásokat folyamatosan vizsgálni kell információbiztonsági szempontból. Amennyiben a változásokkal kapcsolatos figyelési események 30 napig nem jelentenek a tervezettnél magasabb kockázatot, úgy az elfogadott változásokat át kell vezetni a megfelelő dokumentációkon. Amennyiben a megfigyelés időtartama alatt nem tervezett kockázatok jelentkeznek, úgy az engedélyeztetési folyamatot az új kockázatok figyelembe vételével meg kell ismételni.

5. Nem engedélyezhető folyamatok:

a) Nem kérhető és nem engedélyezhető olyan beavatkozás, amely veszélyezteti a Hivatal elektronikus információs rendszerének biztonságát, vagy olyan beavatkozás, amelyhez indokolt védelmi intézkedések aránytalanul magas költségeket és/vagy indokolatlan munkaterhet jelentenek.
b) Nem engedélyezhető olyan protokoll vagy adatátviteli mód, amely alkalmazása esetén nem biztosítható az adatok bizalmasságának és sértetlenségének megőrzése (pl TELNET), vagy amely a rendszer rendelkezésre állását veszélyeztetheti.
c) Nem engedélyezhető olyan alkalmazás használata, amely tudottan sérülékenységet tartalmaz, és nincs vagy nem telepíthető hozzá naprakész biztonsági frissítés.
d) Nem engedélyezhető olyan rendszer használata, amely alkalmas Injection típusú beavatkozásokra vagy olyan hibákat tartalmaz, amely veszélyeztetheti az adatok biztonságát (pl. túlcsordulás, XSS, CSRF, stb.).

6. A nem biztonságos beavatkozások

A Hivatal elektronikus információs rendszereinek biztonságát mérséklő beavatkozás **minden esetben engedélyeztetési eljárás** során végezhető.

Ilyen beavatkozás lehet például, de nem kizárólag:
a) adathordozók használata a hivatali számítógépeken
b) mobil eszközök használata az informatikai hálózatban (laptop, telefon, wifi)
c) alkalmazások telepítése
d) a szokványostól eltérő hálózati munkafolyamatok, protokollok, portok használata
külső rendszerekhez történő kapcsolódás

7. Kockázatelemzés és kezelés az elektronikus információs rendszerekre vonatkozóan

a) A Hivatal mind a hivatali, mind az informatikai folyamataira kockázatelemzést végez a külön dokumentumban írásba foglalt **Informatikai Kockázatelemzési és -kezelési Szabályzatban** meghatározott eljárásrend szerint. Informatikai Katasztrófaelhárítási Terv van.

b) A Hivatal kockázatelemzés és kezelés stratégiáját, eljárásrendjét, a feltárt kockázatokat és a kockázatelemzés eredményét az Informatikai Kockázatelemzési és -kezelési Szabályzat tartalmazza, amely jelen Szabályzattól eltérő, külön dokumentumban kerül meghatározása.

c) Az informatikai kockázatelemzés része a biztonsági kockázatelemzés.

d) A kockázatelemzést minden olyan esetben meg kell ismételni, amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát.

e) A kockázatkezelési tényhelyzet felmérése során meg kell határozni az elektronikus információs rendszerrel kapcsolatos
- védendő értékeket;
- védelmi igényeket és célokat;
- kárérték osztályokat jogszabály alapján.

f) A kockázatelemzés során a homogén kockázatok alapján az elektronikus információs rendszer elemek csoportosítását kell elvégezni; a nem elfogadható mértékű kockázattal bíró rendszerelemek meghatározása mellett; költségbecslést kell végezni a Bizalmasság-Sértetlenség-Rendelkezésre állási elvek alapján a védelmi intézkedés növelésére vagy a kockázat vagy a bekövetkezési valószínűség csökkentésére vonatkozó intézkedési javaslat eredményére tekintettel.

g) A kockázatelemzés során az arányos védelem megvalósításával kell eljárni; az Ibtv.. 6. §-hoz fűzött Indokolásnak megfelelően az a cél, hogy az intézkedések *„költségei hosszútávon arányosak a fenyegetések által okozható károkkal."*

h) Az Informatikai Kockázatelemzési és -kezelési Szabályzat szerint a Vhr. 1. számú melléklet 1. Általános irányelvek alapján, az érintett szervezet az elektronikus információs rendszere, biztonsági osztályba sorolásakor, a Hivatalnak az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit figyelembe véve, a rendszer funkcióira tekintettel kell eljárnia.

i) Az Informatikai Kockázatelemzési és Kezelési Szabályzat minden új kockázat felismerésekor, új rendszerek bevezetésekor, meglévő rendszerek módosításakor, a stratégiában történő változáskor, ezek hiányában legkésőbb évente dokumentáltan felül kell vizsgálni.

j) Az Informatikai Kockázatelemzési és Kezelési Szabályzat nem publikálható, megismerése csak a jogosultak számára engedélyezett. Az Informatikai Kockázatelemzési és Kezelési Szabályzatot az Informatikán, zárt lemezszekrényben kell őrizni. Harmadik fél részére átadni csak a Jegyző írásbeli engedélyével szabad.

k) A Hivatal további – nem informatikai jellegű – folyamatainak kockázatait a Hivatal Ellenőrzési Nyomvonala és Kockázatelemzési Rendszere dokumentum tartalmazza.

l) Külső szolgáltatóval kapcsolatos kockázatelemzési elvárások: Amennyiben a Hivatal munkavégzéséhez külső szolgáltatótól igényel vagy szerez be informatikai fejlesztést vagy szolgáltatást, a szerződésben szerződéses kötelemként érvényesíteni kell a szállított szolgáltatásra vagy fejlesztésre vonatkozó szállítói kockázatelemzést, valamint a hozzá tartozó kockázatelemzési és kockázatkezelési ajánlások dokumentált leszállítását.

8. Az Informatikai Kockázatelemzési és Kezelési Szabályzathoz történő módszertani kapcsolódás.

a) A Hivatal a jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és a nyilvántartása alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók.

b) Az Informatikai Kockázatelemzési és Kezelési Szabályzatban a Vhr. 1. számú melléklet 1. Általános irányelvek alapján az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor, a Hivatalnak az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit figyelembe véve, a rendszer funkcióira tekintettel kell eljárnia.

c) A számításkor a homogén elektronikus információs rendszerelemek kockázatait kellett alapul venni az elektronikus információs rendszerelemek tekintetében; majd a fent felsorolt szempontok (érintett adatkör, lehetséges káresemények, társadalmi-politikai hatás, jogszabályok betartása) alapján 1-5-ig skálán kell a kockázatot meghatározni a Bizalmasság-Sértetlenség-Rendelkezésre állás elvek mentén.

9. Felülvizsgálat

a) Az elektronikus információs rendszer biztonságát érintő változás esetén, illetve új elektronikus információs rendszer bevezetésekor soron kívül meg kell ismételni. A biztonsági szint meghatározását a fenti eseményektől függetlenül legalább háromévenként, szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

b) A Hivatal biztonsági szintbe sorolását a Hivatal vezetője jelen Szabályzat aláírásával jóváhagyja, és jelen Szabályzat betartásával és betartatásával felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért.

10. Intézkedési Terv

a) Az **Ibtv. 18. § (1) és (7) bekezdései** alapján, a Hatóság az érintett szervezetet kötelezheti arra, hogy sérülékenységvizsgálatot végeztessen, valamint a biztonsági eseményt kivizsgáltassa; az érintett szervezet a feltárt hiányosságokról, a sérülékenységek megszüntetésére vonatkozó intézkedési tervről a vizsgálatok lezárását követően tájékoztatja az érintett Hatóságot.

b) Az Intézkedési Tervnek kapcsolódnia kell a biztonsági osztályba és szintbe sorolások felülvizsgálatához.

c) Az Intézkedési Tervben a Hatóság felé mérföldköveket kell meghatározni az elektronikus információbiztonsági stratégia megvalósításához, a védelmi intézkedések megtételéhez.

11. Cselekvési Terv

a) Az Ibtv. 10. § (4) bekezdése alapján: „A 9. § (2) bekezdésében előírt biztonsági szint teljesítése során a szervezetnek lehetősége van az előírt biztonsági szint fokozatos elérésére. Ennek keretében a magasabb biztonsági szint elérésére – minden egyes szintet érintően, a következő magasabb szintre lépéshez - két év áll rendelkezésére."

b) Tekintettel arra, hogy a Jegyző döntése szerint, a Hivatal Üzemeltetési és Informatikai Csoport biztonsági szintje magasabb, mint a Hivatal más területén alkalmazott szervezeti biztonsági szint, ezért önállóan szerkesztett Cselekvési Terv készült. A Cselekvési Tervben dokumentálni kellett a megállapított hiányosságok javítására, tervezett tevékenységeket.

12. Rendszer és szolgáltatás beszerzés, beszerzési eljárásrend

a) A Hivatal önálló Beszerzési Szabályzattal rendelkezik, amely a közbeszerzésekről szóló 2015. évi CXLIII. törvény (Kbt.) hatálya alá tartozó közbeszerzések, továbbá a Kbt. értékhatára alatti áru és szolgáltatások beszerzése, építési beruházások megrendelése esetén alkalmazandó eljárási előírásokat tartalmazzák.

b) A Beszerzési Szabályzatot a közbeszerzési jogszabályok változásának megfelelően a Hivatal frissíti és módosítja.

c) A Hivatallal kapcsolatba kerülő szállítók és szolgáltatók esetén felmerülnek különböző kockázatok lehetősége, például a vállalkozások tulajdonosi köre nem átlátható, az árbevétel vagy jegyzett tőke túl alacsony, nincs megfelelő referencia szerződés, a jó minőségű teljesítés veszélyeztetett, az

alkalmazottak vagy alvállalkozók biztonsági veszélyt jelentenének.

d) A Kbt. értékhatárát elérő közbeszerzések esetén a Hivatal egyértelmű és átlátható követelményeket ír elő az alkalmasság igazolására vonatkozóan.

e) A Kbt. előírja, hogy az Ajánlati felhívásban és annak dokumentációjában részletesen meg kell határozni az ajánlattevők alkalmassági feltételeit, továbbá a beszerzési tárgy objektív műszaki tartalmát.

f) Ehhez a beszerzéseket megelőzően az Üzemeltetési és Informatikai Csoport piackutatást végez a beszerzési tárggyal kapcsolatban, mely biztosítja a beszerzett eszközök rendszerbe történő beillesztéséből adódó kockázatok csökkentését, valamint a becsült érték megállapítását. A beszerzés során nagy súlyt kap a beszerzendő eszközök műszaki specifikációjának a megállapítása, kizárólag ilyen dokumentum alapján történhet a beszerzés.

g) A közbeszerzési és az irodai eljárásokban a benyújtott ajánlatoknak tartalmaznia kell az ajánlattevő alkalmassági megfelelőségét és a megajánlott beszerzési tárgy részletes műszaki paramétereit. Az ajánlatokra vonatkozóan általános előírás, hogy azt a megtétele előtt, más ajánlattevők és külső harmadik személy nem ismerheti meg, a Hivatal bizalmasan kezeli a benyújtott ajánlatok szakmai értékelését.

h) A beszerzésekre vonatkozó döntés előkészítésben kizárólag a Hivatal közbeszerzési gyakorlattal rendelkező munkatársai foglalkoznak, a szakmai tanácsadó szerepet betöltő bíráló bizottság tagjait az ajánlatkérő nevében eljáró Hivatal vezetője vagy a polgármester nevezi ki.

13. Az elektronikus információs rendszerek és eszközök beszerzési eljárása.

a) A Hivatal Beszerzési Szabályzata szerint az Üzemeltetési és Informatikai Csoport által a bíráló bizottságba delegált tag feladatai a következők:

- a beszerzési tárgy pontos megfogalmazása, jellemzőinek részletes meghatározása (pénzügyi, műszaki, piaci paraméterek alapján), a központosított közbeszerzésben a termék (azonosító, cikkszám) konkrét megjelölése, az optimális limitárra és a szerződés lejáratára vonatkozó javaslat meghatározása,
- a lehetséges ajánlattevők alkalmassági / alkalmatlansági ismérveinek részletes összeállítása, a központosított közbeszerzés lehetséges szállítójára és a termék limitárfolyamára való javaslattétel,
- az elbírálás szempontjának / részszempontjainak, értékelési módszertanának leírása,
- részvétel az ajánlati dokumentáció szakmai részének elkészítésében és a részletes szerződési feltételek meghatározásában,
- az ajánlattevőkkel való konzultáció, helyszíni szemle lefolytatása,
- a beérkezett ajánlatok feldolgozásában, az értékelés döntés előkészítésében való részvétel,
- részvétel a központosított közbeszerzés igénybejelentésének adatfelvitelében és a visszaigazolt, valamint az ajánlatkérő által engedélyezett ún. megrendelés elektronikus rögzítésében,
- a szerződés aláírásra való előkészítésében való részvétel,
- az eljárás során készítendő jegyzőkönyvek, tájékoztatások szakmai részének elkészítése,
- a beszerzési döntési javaslat kiterjed a lehetséges szállítók körére, az alkalmassági feltételekre és a lényeges szerződési feltételekre.

b) A lényeges szerződési feltételeknek tartalmazniuk kell:

- az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentáció szállítói átadását, amely tartalmazza: a rendszer, rendszerelem vagy

rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését, a biztonsági funkciók hatékony alkalmazását és fenntartását, a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket;

- az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, ezen belül a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját, a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit, a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához.

c) A lehetséges ajánlattevők kiválasztását megelőzi azok cégkivonatának lekérése és a NAV köztartozásmentes adóslistáján való ellenőrzése.

d) A Kbt. értékhatára alatti áru és szolgáltatások beszerzése, építési beruházások megrendelése esetén a Hivatal vezetője önálló Ajánlati Felhívást küldet ki a lehetséges ajánlattevők részére; a nyertes ajánlattevőt, pedig az előre meghatározott bírálati szempontok szerinti értékelés után határozzák meg.

e) A Hivatalban használt elektronikus információs rendszerek, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök csak az Informatikusok közreműködésével és jóváhagyásával szerezhetők be.

f) Az eszközök, rendszerek, szolgáltatások beszerzését megelőzően az igénylő szervezeti egység részéről pontos, egzakt feladatmeghatározás szükséges a beszerezni kívánt eszközzel vagy szolgáltatással ellátandó feladat funkcióiról, a várható adatmennyiség méretezéséről, a tárolandó adatok köréről és az eszközzel vagy szolgáltatás által végzett feladat várható kockázatairól és azok bekövetkezési valószínűségéről.

g) Nem szerezhető be olyan eszköz, szoftvertermék, rendszer vagy biztonsági megoldás, amely a rendelkezésre álló forrással nem arányosan, potenciális kockázatot jelent a hivatali elektronikus információs rendszerek, eszközök, védelmi megoldások bármelyikének vagy összességének biztonságára, beleértve például, de nem kizárólag, hogy az alkalmazott szoftvertermék már nem támogatott, ismert sérülékenységekkel rendelkezik vagy a beszerezni kívánt rendszer nem támogatott protokollokat, portokat használ adatkommunikációra.

h) Nem szerezhető be olyan rendszer vagy termék, amely olyan járulékos informatikai rendszerek futtatását igényli, amelyek nem támogatottak, vagy az alapkonfiguráció használatával nem működnek. Amennyiben a beszerezni kívánt rendszer vagy eszköz ennek ellenére nem jelent komoly biztonsági kockázatot, úgy a szoftverekre vagy az alapkonfigurációra vonatkozó változáskezelési eljárással történő a szabályok jóváhagyását és módosítását követően a termék beszerezhető.

14. Az elektronikus információs rendszer beszerzésével kapcsolatos szerződéses feltételek

a) Az információ biztonság biztosítása érdekében a fő szerződési előírások, védelmi szabályok a Hivatal részéről, a következők:

- Az ajánlatokban az ajánlattevőknek be kell nyújtaniuk a nemzeti vagyonról szóló 2011. évi CXCVI. törvény 3.§ (1) bekezdésében meghatározott ún. átláthatósági nyilatkozatot, megjelölve abban a vállalkozás tényleges tulajdonosát.

- A beszerzés tárgyától függően szerződéses, annak megerősítését szolgáló elem a Ptk. 6:159. § szerinti kellékszavatosság, a 6:160. § szerinti termékszavatosság, a 6:175. § szerinti jogszavatosság és a Ptk.

6:171. § szerinti jótállás előírása.

- A beszerzés tárgyától függően szerződéses elem a rendszeradaptálás, a beszerzéshez kapcsolódó rendszerkövetés.

- Szükséges szerződéses kötelem, ha a beszerzési tárgy rendelkezik ezzel, az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációi, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírása, a magas és alacsony szintű biztonsági tervek, - ha azzal a szállító rendelkezik - a forráskód és futtatókörnyezet beszállítói átadásának előírása; ha szükséges úgy a licenc jogosultság frissítésének beszerzése.

- Ha alkalmazásra kerül, akkor szállítói kötelezettség, a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereinek dokumentációja, a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához szükséges dokumentáció, a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját leíró dokumentáció, továbbá hogy az adminisztrátori és fejlesztői dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható, azt írásvédett elektronikus adathordozón adja át a szállító.

- Alkalmazandó szállítói kötelezettség, hogy a Hivatal érintett munkatársai számára elvégezze a szerepkörhöz tartozó jogosultságnak megfelelően a rendszerhasználati oktatásokat.

- A szerződések minőség ellenőrzés eredményét kizárólag a Hivatal Üzemeltetési és Informatikai Csoportjának vezetője vagy a Hivatal vezetőjének döntése szerinti más személy igazolhatja le.

- A szerződés teljesítésben résztvevő szakemberek a helyszíni teljesítést / szolgáltatást a Hivatal Üzemeltetési és Informatikai Csoportjának vezetője vagy dolgozója jelenlétében végezhetik el.

- A szerződés teljesítésben résztvevő szakemberek / a szolgáltatást elvégző munkatársai külön-külön titoktartási kötelezettséget vállalnak, e célból készített nyilatkozat aláírásával.

- A szerződő fél a tudomásukra jutott minden nyilvánosság számára nem hozzáférhető információt bizalmasan kezel és kizárólag a másik Fél előzetes írásbeli hozzájárulásával hoz harmadik személy tudomására.

- A vállalkozó a teljesítés során betartja és végrehajtja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban Ibtv.), valamint a végrehajtására kiadott, a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben foglalt előírásokat, valamint a mindenkor hatályos a Megrendelő belső informatikai, adatvédelmi szabályzataiban rögzített és a szolgáltatást bármilyen módon befolyásoló, valamint a munkajogi, munkavédelmi szabályokat.

b) Az elektronikus információs rendszerek beszerzése után, de azoknak a garanciális és a jótállási igényérvényesítés lejárta előtt a Hivatalnak gondoskodnia kell a rendszerekre szóló **üzemeltetési és / vagy Full Service Support szerződések** megkötéséről, amelyek tartalmazzák a rendszer adaptálást, a beszerzéshez kapcsolódó rendszerkövetést.

c) Az elektronikus információs rendszerek biztonságáért felelős személy gondoskodik arról, hogy a beszerzési eljárás eredményeként szállított eszközök, teljesített szolgáltatások használatba vételével együtt a Hivatal érintett munkatársai számára a szerepkörhöz tartozó jogosultságot adjon.

15. Erőforrás igény felmérés, tervezés, nyilvántartás.

a) Az Üzemeltetési és Informatikai Csoport a költségvetés tervezésekor a hivatal ügyviteli folyamatai ellátásához szükséges erőforrásokat egyrészt az egységvezetők által leadott igények, másrészt az osztály által tett megfigyelések, tapasztalatok alapján felméri, javaslatot tesz a beszerzésre, cserére, fejlesztésre szoruló eszközökre, a beszerezni kívánt szoftvertermékekre, fejlesztésekre, auditokra, valamint az információbiztonsággal kapcsolatos beruházásokra, azok költségeire.

b) A javaslatokat a költségvetés-tervezési ügyirat szöveges indoklásában tárgyalja. A kiemelt kockázatokra a szöveges indoklásában felhívja a döntéshozók figyelmét. Költségvetés tervezésekor a különböző szolgáltatásokra, feladatokra tervezett költségeket külön költségvetési sorokra kell tervezni, ezáltal követhetők és számíthatók a szolgáltatások költség-arányai.

c) A költségvetési terv szöveges indoklásában csak a költségvetés-tervezéshez szükséges mértékben tárgyalja a biztonságra kockázatos kérdéseket, a részletes terveket csak döntéshozói utasításra mutatja be.

d) A költségvetési sorokon szerződéssel vagy beszerzési előkészülettel lekötött költségeket, valamint a teljesített kifizetéseket nyilvántartja. A kifizetésekről a beszerzési Szabályzat szerint illetékes szervezeti egységeket tájékoztatja.

16. A Hivatal elektronikus információs rendszerével kapcsolatos alapelvei

A Hivatal az elektronikus információs rendszerével kapcsolatban olyan alapelveket követ, melynek során a rendszer meghatározása, tervezése, fejlesztése, kivitelezése és módosítása során, be tudja tartani:

a) a szolgáltatások elektronikus ügyintézésének minél szélesebb körű biztosítását,
b) az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos működtetését,
c) a személyes adatok fokozott védelmét,
d) az üzletmenet folytonosságot,
e) a biztonsági esemény kezelését,
f) az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárását és értékelését.

17. Biztonságelemzési eljárásrend, folyamatos ellenőrzés, sérülékenységvizsgálat, DRP gyakorlat.

a) **A Biztonságelemzési Eljárásrendet és részeit** a Hivatal jelen Szabályzat keretén belül évente felülvizsgálja és frissíti, melyben értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését.

b) Elkészíti a biztonságértékelés **eredményét összefoglaló jelentést** és megismerteti azokkal a

személyekkel/szervezeti egységekkel akikre ez vonatkozik.

c) A Biztonságelemzési Eljárásrend foglalja magában az alapelveken nyugvó biztonságtervezést,-értékelést és elemzést, továbbá a Biztonságtervezési Szabályzatot.

d) A Hivatal minden olyan beszerzéskor, módosításkor, fejlesztéskor, telepítéskor amely elektronikus információs rendszerek vagy részrendszerek, illetve ilyen jellegű szolgáltatásokra vonatkozik, a beavatkozást megelőzően a **biztonságtervezési -értékelési és -elemzési eljárásrend** szerint megtervezi és megfogalmazza a beszerzendő, módosítandó, fejlesztendő, telepítendő rendszerre vagy szolgáltatásra vonatkozó információbiztonsági kritériumokat és azok teljesülésének, valamint ellenőrzésének menetét.

e) Az eljárásrendet jelen Szabályzat megismertetésével kihirdetettnek minősíti. A Hivatal a biztonságtervezési és -elemzési eljárásrendet jelen Szabályzat felülvizsgálatával egyidejűleg, vagy ha a biztonságtervezés- és elemzési módszertanokban jelentős változás mutatkozik, felülvizsgálja és frissíti.

f) A Hivatal a szervezeten belüli Biztonságelemzési eljárásrendet **három egymásra épülő és egymást kiegészítő ellenőrző részre bontja:**

- megelőző (preventív),
- felismerő (detektív),
- és elhárító (korrektív)

g) A folyamatos belső ellenőrzés célja: a védett rendszer olyan állapota, amelyben annak védelme az összes számításba vehető fenyegetést figyelembe veszi, a rendszer valamennyi elemére kiterjed, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul és annak költségei hosszútávon arányosak a fenyegetések által okozható károkkal.

h) A folyamatos belső ellenőrzés a Hivatal elvárása alapján arra irányul, hogy a rendszer védelménél az adott veszélyek fölötti kontrollra kell helyezni a hangsúlyt és nem feltétlenül a veszélyek bekövetkezésének teljes kizárására, mert az általában megoldhatatlan.

i) Megelőző kontroll közé tartozik a Hivatal dolgozóinak folyamatos informatikai **biztonsági, és rendszerhasználati oktatása**, az informatikai biztonsági elvárások tudatos alkalmazásának biztosítása, a kliens gépek, adathordozók szúrópróbaszerű ellenőrzése.

j) A Hivatalon belüli felismerő, észlelő kontrollok lényege, hogy a folyamatos naplózások, a tűzfal védelem hatékony konfigurálása útján minél hamarabb észleljék egy adott esemény bekövetkeztét, így korlátozva a nem kívánt hatás tovább terjedését (pl. vírusfertőzés), illetve lehetővé téve, hogy az elhárító, helyreállító tevékenység minél előbb fejtse ki hatását.

k) Az informatikai biztonsági elvárásoknak megfelelő, tudatos felhasználói magatartás; mint a rendhagyó események azonnali jelzése, szintén a folyamatos, belső ellenőrzés részét képezik.

l) Az Informatikai biztonságért felelős személy jogosult előzetes egyeztetést követően, a Hivataltól független vállalkozónál ún. **külső sérülékenységvizsgálatot** végeztetni, melynek célja az elektronikus információs rendszerek esetleges gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.

m) Elhárító kontroll: Az elhárító kontrollok szerepe, hogy beavatkozzanak az esetleges rendellenes események folyásába és kiküszöböljék az abból a későbbiek során felmerülő esetleges károkat. Itt a

cél a hibamentes, normálállapot minél előbbi visszaállítása.

n) A visszaállítási idő megfelelő felkészüléssel biztosítható, ezért a Hivatal alkalmazni fogja az **ún. DRP gyakorlatokat.** A DRP gyakorlatok során a Hivatal munkatársainak biztosítani kell a BCP Szabályzatban és Tervben meghatározott minimális üzletmenet-folytonossági célkitűzéseket vagy a Hivatal székhelyén vagy a tartalék oldalon, hogy a Hivatal BCP személyzete megismerje az adottságokat és az elérhető erőforrásokat, valamint a Biztonsági vezető értékelje a tartalék feldolgozási helyszín képességeit a folyamatos működés támogatására.

o) A Jegyző irányításával a Pénzügyi vezető, a Biztonsági vezető és a Hivatal szervezeti egységek vezetői kötelesek a DRP gyakorlatok idején szoros együttműködést és munkamegosztást tanúsítani, ennek során biztosítaniuk kell a munkatársaik segítségével a minimális üzletmenet-folytonossági célkitűzéseket.

p) A Jegyző és az Informatikai biztonságért felelős személy gondoskodik a Hivatal vezetőinek szóló és a minimális üzletmenet-folytonossági célkitűzések, valamint a DRP gyakorlatok követelményeinek megismeréséről, valamint gondoskodnak azok betartatásáról.

q) A Hivatal napi, heti és éves **biztonsági mentéseket végez,** az elektronikus információs rendszer mentéseinek másodlatát az elsődleges helyszínnel azonos módon biztosítja a tartalék oldalon.

r) A DRP Terv, Szabályzat tartalmazza az elsődleges és másodlagos helyszínek kihasználását, elérhetőségét a minimális üzletmenet-folytonossági célkitűzések biztosítása érdekében.

s) A Hivatal az elektronikus információs rendszerek működtetése során olyan szerződéses kötelezettséget biztosít, amelyben **több szolgáltató áll rendelkezésre hasonló szolgáltatás ellátására;** különös tekintettel az irodagépek szállítóira, annak support ellátására, a vezetékes telefon és mobil távközlés, valamint az internet elérhetőség ellátására vonatkozóan.

18. Független értékelők

A Hivatal évente, illetve lehetőségeihez mérten – amennyiben azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik, független értékelővel, vagy értékelő csoporttal értékeli a védelmi intézkedések megfelelőségét.

19. A biztonsági értékelés, Biztonsági teljesítmény mérése

a) A **biztonsági értékelés tartalmazza:**
   - az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedéseket;
   - a biztonsági ellenőrzések eredményességét meghatározó eljárásrendeket;
   - az értékelési környezetet, az értékelő csoportot, az értékelés célját, az értékelést végzők feladatát.

b) A jelen Szabályzatban meghatározott sérülékenységvizsgálati módszertan és gyakoriság szerint ellenőrizni és értékelni kell az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálni kell a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését.

c) Amennyiben a védelmi intézkedések szakmai kompetenciája ezt indokolja, külső független értékelők vagy értékelő csoportok is bevonhatók a védelmi intézkedések folyamatos ellenőrzésére vagy

értékelésére.

d) Az elvégzett tesztek és elemzés alapján **értékelési összefoglaló jelentést, elemzést** kell készíteni, amely összefoglalót, valamint az elemzés alapján megállapított hiányosságok kezelésére készített cselekvési tervet meg kell ismertetni a Jegyzővel, aki az értékelés alapján dönt arról, hogy szükséges-e további személyek értesítése, valamint végrehajtható-e a cselekvési terv.

e) Minden beszerzendő fejlesztendő, módosítandó, telepítendő, valamint alkalmazott rendszert meg kell vizsgálni és **értékelni kell legalább az alábbi információbiztonsági szempontokból:**

- **Injection** az alkalmazás által használt mezőkbe vagy a továbbított adatok közé bevihető-e Injection típusú kódsor (pl SQL, LDAP, stb), nem megbízható adatsor, a mely képes megfelelő jogosítások nélkül végrehajtódni;

- **Broken Authentication and Session Management,** megismerhető-e, feltörhető-e a felhasználó azonosítási vagy munkamenet-kezelési folyamat, amely során az esetleges támadók behatolhatnak, jelszavakat, kulcsokat, tokeneket ismerhetnek meg vagy megismerhetnek, következtethetnek más felhasználói adatokra;

- **Cross-Site Scripting (XSS)** XSS hibák fordulhatnak-e elő, az alkalmazás megbízhatatlan adatokat fogad, és küld a böngészőn keresztül nem megfelelő érvényesítés vagy kiléptetés történik. XSS lehetővé teszi a támadók számára hogy végrehajtson szkripteket az áldozat böngészőjében, amely képes eltéríteni felhasználói munkameneteket, eltorzítani weboldalakat, vagy átirányítani a felhasználót a rosszindulatú webhelyekre;

- **Insecure Direct Object References** a fejlesztés során történik-e olyan objektumhivatkozások meghívása, amelyek jogosítási eljárás nélkül, közvetlenül mutatnak fájlokra vagy könyvtárakra. Az objektumhivatkozások módosításával hozzáférhetővé válhatnak olyan tartalmak, amelyekre az adott felhasználó nincs feljogosítva;

- **Security Misconfiguration** biztonsági szempontból konfigurált-e, megfelelően konfigurált-e az alkalmazás minden komponense, minden komponensre naprakész frissítések kerültek-e telepítésre;

- **Insecure Cryptographic Storage** meg kell vizsgálni, hogy a szenzitív adatokat az alkalmazás megfelelő titkosítással védi-e, az esetleges támadók hozzáférhetnek-e vagy módosíthatnak-e gyengén védett adatokat;

- **Sensitive Data Exposure** meg kell vizsgálni, hogy a szenzitív adatokat az alkalmazás megfelelően védi-e, az esetleges támadók hozzáférhetnek-e vagy módosíthatnak-e gyengén védett adatokat;

- **Failure to Restrict URL Access** hozzáférés ellenőrzés nélkül lekérdezhetők-e az adott honlapok vagy alkalmazások által tárolt fájlok, könyvtárak az URL cím módosításával;

- **Missing Function Level Access Control** meg kell vizsgálni, hogy az alkalmazás tartalmaz-e különféle hozzáférési jogosítási szinteket, vagy a felhasználói azonosítással egyébként nem látható de végrehajtható funkciók ténylegesen végrehajthatók-e megfelelő felhatalmazás nélkül is;

- **Cross-Site Request Forgery (CSRF)** az alkalmazás tartalmazhat-e olyan sérülékenységet, amely során a rendszerbe bejelentkezett felhasználók adatai, cookie-k, jogosításhoz szükséges információk, stb. hamisított http kérésen keresztül megismerhetővé válhatnak;

- **Using Known Vulnerable Components** az alkalmazás tartalmaz-e ismert sebezhetőségekkel futó összetevőket (pl. könyvtárak, keretrendszerek, stb). Az ilyen rendszereket általában teljes jogosultsággal futtatják, aminek az esetleges sebezhetősége adatvesztéshez vagy a szerver feletti irányítás átvételére is alkalmas lehet;

- **Unvalidated Redirects and Forwards** a Webes alkalmazások gyakran átirányítják, és továbbítják a felhasználókat más oldalakra és honlapokra, de megbízhatatlan adatok alapján határozza meg a cél oldalakat. A megfelelő érvényesítés nélkül a támadók át tudják irányítani az áldozatokat adathalász vagy rosszindulatú webhelyekre, vagy jogosulatlan oldalakhoz történő hozzáféréshez;

- **Insufficient Transport Layer Protection** az alkalmazás megfelelően védett csatornán történik-e. A hálózati forgalom védett-e , titkosított-e, elégséges védelmet nyújt-e az adathozzáférés vagy módosítás ellen. Az alkalmazás támogat-e lejárt vagy érvénytelen tanúsítványokat, helyesen használja-e azokat;

- **Overflow (Buffer, stack)** az alkalmazás védett-e buffer vagy stack overflow ellen, használ-e olyan programozástechnikai megoldásokat, amelyek nem kezelik a túlcsordulás okozta problémákat;

f) Alkalmazások mentése az alkalmazásról és adatairól készíthető-e biztonsági mentés, és a mentés teljes körűen, működőképesen, teljes adattartalommal visszaállítható-e a Hivatalban alkalmazott mentési metódussal, vagy saját mentési megoldást alkalmaz (pl. export);

g) **Felelősségek szétválasztása** az alkalmazás képes-e a felelősségeket olyan módon szétválasztani, hogy akár rendszer-üzemeltetési, fejlesztési, akár üzletmenet szempontjából egymással összeférhetetlen szerepek egy felhasználó által ne legyenek hozzáférhetők. Teljes ügymenetet egy felhasználó ne tudjon megfelelő ellenőrzési és jóváhagyási folyamat beiktatása nélkül véghezvinni;

h) **Sikertelen bejelentkezési kísérletek** az elektronikus információs rendszer vagy rendszerelem paraméterezhető-e úgy, hogy meghatározott esetszám korlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. Amennyiben a sikertelen bejelentkezési kísérletekre felállított esetszám korlátot – 3 - a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet;

i) **Rendszerhasználat jelzése** az érintett elektronikus információs rendszer alkalmas a Hivatal által meghatározott, rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küldeni a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelzi, hogy:

  - a felhasználó az érintett szervezet elektronikus információs rendszerét használja
  - a rendszer használatot figyelhetik, rögzíthetik, naplózhatják
  - a rendszer jogosulatlan használata tilos, és **büntetőjogi vagy polgárjogi felelősségre vonással jár**
  - a rendszer használata egyben a **felhasználó előbbiekbe történő beleegyezését is jelenti.**

j) Az elektronikus információs rendszer alkalmas arra, hogy a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.

k) Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén képes-e kijelezni a ~~a~~ rendszer használat feltételeit, mielőtt további hozzáférést biztosít, biztosít-e leírást az engedélyezett felhasználásáról, amennyiben felügyelet, adatrögzítés vagy naplózás történik, jelzi-e, hogy ezek

megfelelnek az adatvédelmi szabályoknak.

l) Egyidejű munkaszakasz kezelés az elektronikus információs rendszer képes-e meghatározott számra (legfeljebb 2) korlátozni az egyidejű munkaszakaszok számát, a meghatározott fiókok vagy fiók típusok számára külön-külön;

20. Sérülékenység teszt, frissítések

a) A Hivatal évente, illetve pénzügyi lehetőségeihez mérten – amennyiben azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik – minden a Hivatal üzemeltetésében lévő kritikus rendszerelemet érintő vagy az elektronikus információs rendszert érintő változás vagy biztonsági kockázat felmerülése esetén a kockázatok kezelését követően **külső szakértővel, vagy sérülékenységvizsgálati eszközök és technikák alkalmazásával sérülékenységvizsgálatot végeztet.**

b) A Hivatal lehetőségeihez mérten, amennyiben a sérülékenységvizsgálathoz teszteszközt használ, a teszteszköz kiválasztásakor ügyel arra, hogy az eszköz sérülékenység feltáró képessége könnyen bővíthető legyen az ismertté váló sérülékenységekkel.

c) Sérülékenységvizsgálat esetén, a Hivatal az integrált elektronikus információs rendszereihez **elkülönített teszt környezetet bocsát rendelkezésre, - amennyiben lehetőségei azt megengedik -** amely alkalmas a hibák, sebezhetőségek, kompatibilitási problémák és szándékos károkozásra utaló jelek keresésére. A teszt rendszerhez **privilegizált hozzáférést kell** biztosítani a sérülékenységvizsgálatot végző számára az Informatikusok felügyelete mellett.

d) Sérülékenységvizsgálatok során feltárt hiányosságok kezelése

- A sérülékenységvizsgálat során feltárt hibákról, nem megfelelő konfigurációs beállításokról a Hivatal kimutatást készít vagy készíttet, végrehajtja az ellenőrzési listákat és tesztelési eljárásokat felméri a sérülékenység lehetséges hatásait, elemzi a sérülékenység teszt eredményét és megosztja a sérülékenység teszt eredményét a szervezet által meghatározott személyekkel és szerepkörökkel.

- Amennyiben a feltárt sérülékenységek a kockázati besorolás szerint kritikusak, vagy beavatkozást igényelnek, úgy gondoskodik a feltárt sérülékenységek haladéktalan javításáról.

- Lehetősége szerint új elektronikus információs rendszer beállítását megelőzően a teljes rendszert független, külső (úgynevezett fekete dobozos) sérülékenységvizsgálatnak veti vagy vetteti alá, mely során a fejlesztőtől/szállítótól megköveteli a pozitív eredményű (csak a szervezet által elfogadható maradványkockázatokat tartalmazó), legalább fokozott garanciaszintű rendszerértékelés vagy tanúsítás meglétét.

e) Felfedhető információk

Hivatal a külső sérülékenységvizsgálatok, IT biztonsági szolgáltatások vagy **sérülékenységvizsgálati teszt** eszközök használatakor meghatározza vagy meghatároztatja, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javításokat hajt végre.

21. Rendszerbiztonsági terv

A Hivatal az általa üzemeltetett kritikus elektronikus információs rendszerekhez önálló dokumentumba foglalt **Rendszerbiztonsági Terveket készíttet, mely tartalmazza:**

- A rendszer átfogó ismertetését
- A hardver szoftver környezetet
- A rendszer felügyeletét
- A telepítés leírását, javítását
- Biztonsági követelményeket a hardver és a szoftver komponensekre
- Adatcsere követelményeket
- Kockázatokat
- Hozzáféréseket
- Felhasználói jogosultságokat
- Használat során elvégzendő üzemeltetési feladatokat
- A rendszer kivonása esetén felmerülő feladatokat

22. Beszerzések, szállítóval szemben támasztott követelmények; (funkciók – protokollok – szolgáltatások)

a) Az engedélyezett funkciókat, portokat, protokollokat, szolgáltatásokat és szoftvereket rendszeresen felül kell vizsgálni az alábbi esetekben:
   - jelen Szabályzat felülvizsgálatakor
   - új igények bejelentésekor (változáskezelés)
   - új sérülékenységek ismertté válásakor
   - új, alkalmazható technológiák megismerésekor (tesztelést követően)

b) A felülvizsgálat során meg kell határozni és ki kell zárni, vagy le kell tiltani a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.

c) A Hivatal elektronikus információs rendszerei vagy azok részei beszerzésekor, a rendszerek működéséhez szükséges szolgáltatások és beszerzések alkalmával a Szabályzatban meghatározott szerződéses kötelmeket kötelezően bele kell foglalni a szolgáltatóval, fejlesztővel, vállalkozóval kötött szerződésbe.

d) Jogszabályi kötelezettség.

- A beszerzési és közbeszerzési eljárásokban beszerzett áru és szolgáltatás műszaki tartalmának meghatározásakor a Hivatal köteles figyelembe venni az Ibtv.-ben foglalt követelményeit; továbbá a potenciális ajánlattevőkkel kapcsolatban meghatározott alkalmassági feltételeket szintén biztosítani kell az Ibtv.-ben foglalt követelményeket.

- Az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az Ibtv.-ben foglaltak szerződéses kötelemként a szolgáltatóval szemben teljesüljenek.

- Ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az Ibtv.-ben foglaltak szerződéses kötelemként teljesüljenek.

e) Egyéb tartalmi kötelezettségek

- Az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködő vállalkozóval vagy szállítóval kötött

szerződésben, valamint a Hivatal számára adatkezelési vagy az adatfeldolgozási tevékenységben közreműködő vagy **a Hivatal számára külső szolgáltatást nyújtó vállalkozóval vagy szállítóval kötött szerződésben, szerződéses kötelezettségként meg kell követelni,** hogy a szolgáltatási szerződés alapján az igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek **az érintett szervezet elektronikus információbiztonsági követelményeinek.**

- A leszállított termékek nem tartalmaznak olyan megoldásokat, amelyek különféle ismert sebezhetőséget tesznek lehetővé (pl. SQL injection, XSS, CSRF), ellenőrizetlen vagy nem biztonságos hivatkozásokat tartalmaznak, vagy lehetővé teszik az authentikáció egyszerű kikerülését, megismerését, feltörését. A jogosított rendszereknek úgy kell működniük, hogy a jogosításhoz kötött tartalmak ne legyenek hozzáférhetők a megfelelő jogosítás hiányában, például a hivatkozás közvetlen megismerése által.

f) A Beszerzésekkel kapcsolatos követelmények csoportjai.

- Az elektronikus információs rendszer egésze, részei leszállításával vagy a szolgáltatás teljesítésével kapcsolatban meg kell határozni az elfogadási kritériumokat, mind a rendszer funkcionalitása, mind az elvárt nem funkcionális követelmények, mind pedig a rendszer biztonsága vonatkozásában.

- Funkcionális és nem funkcionális követelmények. A funkcionalitással kapcsolatos és a nem funkcionális kritériumokat a fejlesztést, beszerzést igénylő szervezeti egység határozza meg, teljes körűen. A funkcionalitással és nem funkcionális követelményekkel kapcsolatos elvárásokat a szerződés mellékletében definiálni kell.

- Biztonsági kritériumok. A biztonsági kritériumok minden esetben a szállítandó rendszer és komponensei specifikumában határozhatók meg. A fentiekben meghatározott követelményeknek való megfelelésen túl a rendszerspecifikus megfeleléseket a szerződésben definiálni kell. A biztonsági megfelelőség külső auditorral ellenőriztethető.

- Átadás-átvétel. A rendszer vagy komponensei telepítését az eszköz átadás-átvételi eljárása, majd sikeres átadás-átvétel esetén az üzembeállítása követi. A megfelelő teljesítést követően az átadás-átvételt jegyzőkönyvben vagy teljesítési igazolással kell dokumentálni.

g) A Hivatal elektronikus információs rendszerének vagy rendszerelemének, szolgáltatásának vagy komponensének beszerzésekor az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) **szerződéseiben követelményként meg kell határozni az alábbiakat:**

- A funkcionális biztonsági követelményeket.

- A funkcionalitás biztonsága vonatkozásában meg kell határozni a rendszerbe bevihető adatok körét, ki kell zárni olyan adatok bevihetőségét, amelyek túlcsordulást vagy nem kívánt (pl. injection típusú) kódok bevitelét eredményezhetik. Ellenőrizni kell a bevinni kívánt adatok konzisztenciáját, valós értékeit.

- A garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint).

- Ha a fejlesztés vagy a rendszerbeszerzés során harmadik féltől származó szoftverelemek kerülnek beszerzésre, biztosítani kell a harmadik féltől való frissítések beszerzését a rendszer életciklusára, élettartamára.

- A harmadik féltől beszerzett termékek (pl, nyílt forráskódú szoftverek) esetén gondoskodni kell arról, hogy a kód a gyártó által támogatott verzióban és módosítások nélkül fusson, hogy a későbbi biztonsági frissítések támogatott módon lefussanak.

- A műszaki biztonsággal kapcsolatos dokumentációs követelményeket.

- Az információ biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket.

- Az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

- Amennyiben a kódban a gyártó által nem támogatott változtatások kerülnek bevezetésre, úgy a dokumentációban meg kell követelni a forráskód módosításainak részletes magyarázatát, és megoldását, hogy a biztonsági frissítések lefuttatását követően is a szükséges módosítások átvezethetők legyenek;

- Kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás vagy az abban felhasznált komponensek biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit az Hivatal által meghatározott kapcsolattartó személyeknek.

- Ne használjon ismert sérülékenységeket tartalmazó rendszereket javítás nélkül.

- A leszállított termékekhez a Vállalkozó / Eladó / Szolgáltató köteles üzletmenet-folytonossági és katasztrófaelhárítási ajánlást készíteni, amelyben meghatározzák a kritikus folyamatok kiváltásának és a katasztrófaesemény helyreállításának lépéseit.

- Egypontos hiba kezelését, miszerint a leszállított termékek nem tartalmazhatnak olyan megoldásokat, amelyekben lehetséges SPOF (Single Point of Failure), az elektronikus rendszerek bővítésekor az egyedi hibapont (SPOF) elkerülése, növeli a stabilitást abban az esetben, ha az eszközök valamelyike meghibásodna, vagy elérhetetlenné válna.

- A Vállalkozó / Eladó / Szolgáltató, akkor lehet szerződő fél, ha átlátható szervezetnek minősül a nemzeti vagyonról 2011. évi CXCVI. törvény 3. § (1) bekezdése alapján, így különösen: tulajdonosi szerkezete, a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvény szerint meghatározott tényleges tulajdonosa megismerhető, nem minősül a társasági adóról és az osztalékadóról szóló törvény szerint meghatározott ellenőrzött külföldi társaságnak; a Szerződés aláírásával egyidejűleg cégszerűen aláírt ún. átláthatósági nyilatkozatot ad át.

- A Vállalkozó / Eladó / Szolgáltató / bejelenti a teljesítésben résztvevő szakemberei nevét és azonosító okmányuk számát.

- A biztonsággal kapcsolatos dokumentációs követelmények teljesítése miatt a Vállalkozó / Eladó / Szolgáltató / teljesítésben résztvevő szakemberei a helyszíni teljesítést / szolgáltatást a Polgármesteri Hivatal Jegyzői Iroda Üzemeltetési és Informatikai

Csoportjának informatikus dolgozója jelenlétében végezhetik el.

- A szerződésben rendelkezni kell az információbiztonsági szempontból bizalmas vagy szenzitív információkat tartalmazó dokumentumok elkészítésének, terjesztésének, szállításának, átadásának paramétereiről. A dokumentumokkal kapcsolatban titoktartási kötelezettséget kell vállaltatni a Vállalkozó / Eladó / Szolgáltató képviselőivel.

- Az információbiztonsági szempontból bizalmas vagy szenzitív információkat tartalmazó hivatali dokumentumok csak a szerződésben meghatározott személy részére adható át.

- Amennyiben a szerződés távoli karbantartási lehetőséget is tartalmaz a vállalkozó által a távoli karbantartásra használt információs rendszer legalább a szervizelendő vagy karbantartandó rendszerrel azonos biztonságú kell, hogy legyen. A karbantartás csak előzetes rendszer-beavatkozási kérelem alapján, azonosított és hitelesített megoldással csak a karbantartás időszakára engedélyezhető.

- A leszállított termékekhez, nyújtott szolgáltatáshoz a Vállalkozó / Eladó / Szolgáltató köteles üzletmenet-folytonossági és katasztrófaelhárítási ajánlást készíteni, amelyben meghatározzák a kritikus folyamatok kiváltásának és a katasztrófaesemény helyreállításának lépéseit.

- Amennyiben a rendszer működtetésére az üzletmenet folytonosságot is érintő szolgáltatási szerződés is megkötésre kerül, úgy a szerződésben pontosan definiálni kell Vállalkozó / Eladó / Szolgáltató részéről az érintett szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősség köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is.

- Mentési terv. A Vállalkozó / Eladó / Szolgáltató leszállítandó termékekre vonatkozóan szállító mentési tervet készít, amelyben meghatározza a rendszer mentési fázisait, lépéseit, a mentendő adatok helyét, a mentés típusát (pl. export, dump, stb.) ajánlást tesz a különböző elemek mentési gyakoriságára.

- Biztonsági teszt. A Vállalkozó / Eladó / Szolgáltató ajánlást tesz az általa szállítandó termékre vonatkozó biztonsági tesztre, amelyen a Megrendelőnek módosítási joga van. A módosításhoz a Megrendelőnek lehetősége van külső szakértőt igénybe venni, valamint a leszállított rendszert külső szakértővel megvizsgáltatni, és a rendszer működését ellenőrizni.

- A beszerzett szoftvertermékek, rendszereszközök, rendszerszoftverek teljes funkcionalitására vonatkozó Rendszerbiztonsági tervet kell készítenie a Vállalkozónak. A rendszerbiztonsági tervnek tartalmaznia kell a jelen dokumentumban meghatározott követelményeket. Ez esetben az elektronikus információs rendszer rendszerbiztonsági tervében dokumentálni kell a távoli karbantartási és diagnosztikai kapcsolatok létrehozására és használatára vonatkozó szabályokat és eljárásokat.

- Adminisztrátori kézikönyv. A szerződésben meg kell határozni, hogy a Hivatal szerződésben definiált kapcsolattartója számára (kizárólag az ő számára) a teljesítéskor meghatározott példányszámban (legalább 2 példány) át kell adni az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó rendszer adminisztrátori kézikönyv dokumentumot, amely tartalmazza legalább, de nem kizárólag:
    - a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálására,

telepítésére és üzemeltetésére vonatkozó minden releváns információt, sorrendiséget, függőségeket,
- a biztonsági funkciók hatékony alkalmazását és fenntartását,
- a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

- Felhasználói kézikönyv. A beszerzésekkel kapcsolatos szerződésben meg kell határozni, hogy a Hivatal szerződésben definiált kapcsolattartója számára (kizárólag az ő számára) a teljesítéskor meghatározott példányszámban (legalább 2 példány) át kell adni az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó rendszer felhasználói dokumentációt, amely tartalmazza legalább, de nem kizárólag:
  - a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját, kivételeket, kivételek kezelését,
  - a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit,
  - a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához
  - A szerződés teljesítésének biztosítékait, kötbérek előírásait, a jótállási és garancia követelmények szerződéses alkalmazását.

- A Hivatal a teljesítés igazolását követően, a számla ellenértéket átutalással teljesíti a kiállított számla kézhezvételét követően, a szerződésben/megrendelőben foglaltak szerint.
- Hiánytalan minőségi teljesítés esetén a Hivatal képviselője teljesítés igazolást állít ki. A teljesítés eredményét kizárólag a Hivatal Üzemeltetési és Informatikai Csoportjának vezetője igazolhatja le.

23. Az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírások.

a) Éles üzemi környezet. Elektronikus információs rendszer fejlesztésekor a szerződésben definiálni kell, hogy a fejlesztett rendszer milyen paraméterekkel (pl. virtualizációs paraméterek, LUN stb.), milyen rendszerben kerül bevezetésre és éles üzemű üzemeltetésre.

b) Fejlesztési környezet. Elektronikus információs rendszer fejlesztésekor a szerződésben definiálni kell, hogy a fejlesztett rendszer fejlesztése milyen infrastruktúrán történik. A fejlesztés soha nem történhet az éles üzemi rendszeren.

A fejlesztés során gondoskodni kell arról, hogy az éles üzemi adatokhoz kizárólag olyan személyek férnek hozzá, akik a megfelelő jogosítványokkal rendelkeznek. Az éles üzemi adatokhoz és azok másolatához nem férhetnek hozzá a fejlesztők és olyan üzemeltetők, akik nem rendelkeznek jogosítvánnyal az érintett adatok megismerésére.

c) Teszt környezet. Elektronikus információs rendszer fejlesztésekor a szerződésben definiálni kell, hogy a fejlesztett rendszer esetén minden alkalommal biztosítani kell külön teszt környezetet, amely működése és paraméterei azonosak az éles üzemi környezetével, eltérés kizárólag a tesztelés célját meghatározó elemekben lehet.

A tesztelés során definiálni kell a teszt környezetbe feltöltött adatokat, azok állapotát. Tesztelési céllal a

hatékony és életszerű tesztelés érdekében importálhatók éles üzemi adatok, de csak akkor, ha azokhoz kizárólag olyan személyek férnek hozzá, akik az éles üzemi rendszerben is ugyanazokkal a jogosítványokkal rendelkeznek.

Az éles üzemi adatokhoz és a teszteléshez feltöltött éles üzemi adatok másolatához nem férhetnek hozzá a fejlesztők és olyan üzemeltetők, akik nem rendelkeznek jogosítvánnyal az érintett adatok megismerésére.

d) oktatási környezetet.
Az oktatási környezetnek funkcionalitásában azonosnak kell lennie az éles üzemi környezet funkcionalitásával, a beállításokban csak olyan paraméterekben lehet eltérés, amelyek alapján megkülönböztethető az éles üzemi és az oktatási környezet.

Oktatási célra a hatékony és életszerű oktatás érdekében importálhatók az éles üzemi adatok, de csak akkor, ha azokhoz kizárólag olyan személyek férnek hozzá, akik az éles üzemi rendszerben is ugyanazokkal a jogosítványokkal rendelkeznek. Az oktatáshoz feltöltött éles üzemi adatok másolatához nem férhetnek hozzá a fejlesztők és olyan üzemeltetők, akik nem rendelkeznek jogosítvánnyal az érintett adatok megismerésére.

Az oktatást ilyen esetben csak olyan személy (superuser) végezheti, aki ismeri a rendszer működését, és rendelkezik jogosítvánnyal az éles üzemi adatok rendszerszintű megismerésére.

24. Teljesítés utáni rendszerkövetés.

Az elektronikus információs rendszerek beszerzése után, de azoknak a garanciális és a jótállási igényérvényesítés lejárta előtt a Hivatalnak gondoskodnia kell a rendszerekre szóló üzemeltetési és / vagy Full Service Support szerződések megkötéséről, amelyek tartalmazzák a rendszer adaptálást, a beszerzéshez kapcsolódó rendszerkövetést.

25. Beszerzések, rendszerelemek beállítása.

Az elektronikus információs rendszerek egészének, részeinek **beszerzésével, szolgáltatásával kapcsolatos szerződésekben definiálni kell** az alábbi kötelmeket:

a) A Hivatal előírja, hogy az elektronikus információs rendszer hardver elemeinek és a hozzájuk tartozó rendszerszoftverek beszerzése esetén egy előzetes specifikálás során kell meghatározni a beszerezni kívánt eszköz:
   - biztonsági beállítási követelményeit,
   - sérülékenység és behatolás elleni védelmi szintjét,
   - az adott funkció teljesítéséhez szükséges biztonságtechnikai jellemzőket (protokollok, szolgáltatások, stb.).

b) Az elektronikus információs rendszer hardver elemeinek és a hozzájuk tartozó rendszerszoftverek telepítését végző személy biztosítja, hogy a telepített eszközön az előző pontban meghatározott követelmények teljesülnek. A fenti követelményektől csak az Üzemeltetési és Informatikai Csoportvezető hozzájárulásával lehet eltérni.

c) A Központi rendszer hardver elemeinek és a hozzájuk tartozó Rendszerszoftverek **telepítését** az Informatikus munkatársa a Szállító instrukciói és dokumentációi alapján egyedül vagy a Szállítóval közösen végzi.

d) A szállítói szerződésben ki kell kötni, hogy a biztonsági hiányosságokra kiadott **programfrissítésekről** a Szállító adott határidőn belül értesíti a Hivatalt. A programfrissítések telepítésének a tesztelést követő lehető leggyorsabb végrehajtása az Informatikusok feladata.

e) **A tesztet a fejlesztő végzi el** az általa készített biztonságértékelési terv alapján, amely tartalmazza a fejlesztéshez illeszkedő módon egység-, integrációs-, rendszer-, vagy regressziós tesztelést, és ezt értékelje ki a Hivatal által meghatározott lefedettség és mélység mellett. Dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat és ismertesse a biztonsági tesztelés és értékelés eredményeit és javítsa ki a biztonsági tesztelés és értékelés során feltárt hiányosságokat.

f) Követelményként szükséges rögzíteni, hogy a telepítés során az eszköz naplózási paramétereit (ha vannak ilyenek) olyan módon kell beállítani, hogy a naplózás alkalmas legyen a biztonsággal kapcsolatos események regisztrálására, az adott eszközre elérhető legteljesebb mértékben. A naplózandó eseményekre a Szállító ajánlást tesz, az Informatikusoknak, akik jogosultak a naplózandó események körének megváltoztatására, bővítésére.

g) A számítástechnikai eszköz telepítésének része az ellenőrzés, amelynek eredményét, azaz hogy az eszköz a meghatározott biztonsági követelményeknek eleget tesz, az Informatikus–a rendszer átvételekor, a Tesztelési jegyzőkönyvben rögzíteni köteles.

h) A Hivatal az üzemmenet folytonosság szempontjából kritikus számítástechnikai eszközt vagy rendszert (pl. szerver, operációs rendszer, adatbázis-kezelő) csak akkor állít üzembe, ha az azon az eszközön elvégzett technikai vizsgálatok (tesztkörnyezetbeli funkcionális és terheléses tesztek) nem mutatnak ki súlyos hibát. A tesztelés módját, eredményeit az Informatikus a Tesztelési Jegyzőkönyvben dokumentálja.

i) A harmadik személyektől igénybe vett informatikai szolgáltatások esetében a szolgáltatási szerződésben definiálni kell a szolgáltató hozzáférési jogosultságát, annak ellenőrizhetőségét. A szolgáltató adatszintű hozzáférését minden szerződésben tiltani kell.

j) A szolgáltatóval jelen Szabályzatot, illetve minden adatvédelemmel, tűzvédelemmel, behatolásvédelemmel, objektumvédelemmel, informatikai biztonsággal, üzletmenet-folytonossággal, katasztrófaelhárítással, mentéssel kapcsolatos szabályozást ismertetni kell, a szerződésbe minden alkalommal bele kell fogalmazni, hogy a szolgáltató az adott Szabályzatokat ismeri, a szolgáltatások nyújtásakor mindenben aszerint jár el.

26. Külső elektronikus információs rendszerek szolgáltatásai, a Szolgáltató alkalmazottaival kapcsolatos előírások.

a) Elő kell írni, hogy **ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre,** aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést a Hivatal kijelölt kapcsolattartójának.

b) Folyamatosan ellenőrizni kell a szerződő fél személybiztonsági követelményeknek való megfelelését.

c) Amennyiben a Hivatal a feladatellátáshoz külső elektronikus információs rendszerek szolgáltatását veszi igénybe, a szerződésben definiálni kell az érintett szervezet felhasználóinak feladatait és kötelezettségeit.

XI. Fizikai és környezeti védelmi intézkedések.

A fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.

27. A Hivatal épületeibe történő be- és kiléptetés

a) Fizikai védelmi intézkedésnek minősül a Hivatal épületeibe történő be- és kiléptetés, valamint az épületekben tartózkodás. Ennek ellenőrzése hivatali időben a portaszolgálat feladata. Az őrzési szolgálati idő: huszonnégy órában folyamatosan;

b) Az épületbe érkező ügyfelek és látogatók beléphetnek. A belépő személyeket a belépési pontokon ellenőrizni és azonosítani kell, meg kell vizsgálni a belépés jogosultságát.

c) Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre, valamint arra, hogy e fejezet rendelkezései az adott létesítmény bárki által szabadon látogatható, vagy igénybe vehető területeire nem vonatkoznak.

d) A nevezett **eljárásrendet** jelen Szabályzatra vonatkozó előírások szerint és gyakorisággal kell felülvizsgálni és szükség esetén frissíteni.

d) Munkaidőn kívül riasztó rendszerrel biztosított, zárt vagy portaszolgálat által felügyelt őrzést alkalmaz a Hivatal.

28. A belépőkártyákra vonatkozó szabályok.

a) A Hivatal dolgozói belépőkártyával rendelkeznek.

b) A személyre szabott proximity kártyákat az Üzemeltetési és Informatikai Csoportvezető, vagy az általa felhatalmazott személy személyesíti meg, és adja ki a jogosultak számára az Informatikai Csoport Okiratminták alapján. A felek az átadást, átadás-átvételi jegyzőkönyvvel hitelesítik.

c) A jegyzőkönyv tartalmazza az átadó és az átvevő személy nevét, a szervezeti egységüket, az átadás-átvétel tényét, idejét, helyét, továbbá a személyre szóló kártya sorszámát, tartalmaz továbbá egy nyilatkozatot az átvevő részéről, amelyben kijelenti, hogy tudomásul veszi a kártya használatából eredő kötelességeit és felelősségeit.

d) A kártya jogosultságokat az Üzemeltetési és Informatikai Csoportvezető állítja be a megfelelő jogosítványok alapján, az eljárásrend szerint. A jogosításokról, valamint a kiadott eszközökről a beléptető rendszer részletes elektronikus nyilvántartást vezet.

e) Az Üzemeltetési és Informatikai Csoportvezető a nyilvántartás alapján az informatikai szervezetben vagy a belépésre jogosított személyek körében történő változások esetén, illetve meghatározott bejelentések alkalmával haladéktalanul, de minden felülvizsgálatot követő egy éven belül

dokumentáltan felülvizsgálja a belépésre jogosult személyek listáját, eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt, megvonja a kompromittálódott, elvesztett, sérült azonosító eszközök. valamint a belépési jogosultságaikat vesztett felhasználók belépési jogait.

f) A kártya csak rendeltetésszerűen használható. A kártyával történő belépések és zónában tartózkodások csak indokolt esetben, csak a munkavégzéshez szükséges időtartamban a munka elvégzéséig történhetnek.

g) A fokozott és a kiemelt zónákban felügyeletet vállaló és/vagy a be- és/vagy kilépést engedélyező jogosultsággal rendelkező személy feladata az állandó belépési engedéllyel nem rendelkező személyek zónában tartózkodása alatt a személyek felügyelete.

h) A kártya elvesztéséért, valamint a kártya adatainak kompromittálódásáért, illetve a kártyával történő ajtónyitások alkalmával történő további személyek jogosulatlan belépéséért kártérítési felelősséggel tartozik.

i) Átvevő személy kártya elvesztésekor, megrongálódásakor, megsemmisülésekor, kompromittálódásakor vagy a belépési jogosultság elveszítésekor (pl. munkaviszony megszűnése, tartós távollét, stb.) az eseményt haladéktalanul jelezni köteles az Üzemeltetési és Informatikai Csoportvezető felé, aki a kártya jogait haladéktalanul visszavonja, egyidejűleg ellenőrzi, hogy az esemény óta történt-e esetleges visszaélés az azonosító kártyával.

j) A jogosultság megszűnésekor az átvevő köteles a kártyát haladéktalanul visszajuttatni az Üzemeltetési és Informatikai Csoportvezető részére.

k) A fokozott biztonsági zónában munka végeztével utoljára csak olyan munkatárs maradhat, aki jogosult a biztonsági zóna zárására. Ezen zónák bezárásáról és a szükséges védelmi intézkedések megtételéről a területet utoljára elhagyó munkatárs gondoskodik.

l) Az élőerős védelmet, portaszolgálatot a Hivatal saját foglalkoztatott személyek útján biztosítja.

m) A portaszolgálat az ügyfél és vendég be- és kiléptetését papír alapon vezetett Beléptetési Naplóban, folytonosan, sorszámozott módon rögzíti. A rögzítést megelőzően kell elvégezni az ügyfél, vendég azonosítását, majd ezt követően a Beléptetési Naplóban kell rögzítenie az ügyfél, vendég nevét, a személyazonosító okmány számát, megjelölését, a beléptetés idejét, a látogatás okát, célját.

n) Különösen indokolt esetben (pl: személy- és vagyonbiztonság megóvása, illetve jelentős kár megelőzése érdekében) a fokozott, illetve a kiemelt biztonsági zónákban is az erre jogosult személyek azonosító kártya nélkül is beléphetnek, amennyiben az azonosító kártyával rendelkező munkatársak vagy az azonosító eszközök nem érhetők el a szükséges időn belül.

o) Rendkívüli vagy különösen indokolt esetben a portaszolgálat számára leadott, ott elzártan tárolt kulcs használatával lehetséges. A kulcs elhelyezése az Üzemeltetési és Informatikai Csoport körbélyegzőjével és a csoportvezető aláírásával hitelesített borítékban történik.

p) A kiemelt és fokozott védelemmel ellátott informatikai célú helyiségekbe állandó belépési jogosítvánnyal nem rendelkező belső vagy külső munkatársak belépése és zónában tartózkodása csak különösen indokolt esetben (pl. tervezett karbantartás, fejlesztés külső szakértők részvételével, nem tervezett események: üzletmenet folytonosságot veszélyeztető esetek hibaelhárítási vagy katasztrófaelhárítási feladatok) a zónára érvényes jogosítványokkal rendelkező informatikai munkatárs felügyeletével történhet.

q) A kiemelt és fokozott védelemmel ellátott helyiségekben a kártyával nem azonosított, azzal nem rendelkező személyek beléptetésének naplózására az Üzemeltetési és Informatikai Csoportvezető által átadott Belépési Naplót kell vezetni.

29. Biztonsági zónák.

a) Hivatalban épületeiben a fizikai hozzáférések felügyelete, védelme és a környezeti károk eltérő szintű kockázati kitettsége miatt eltérő biztonsági zónákat hoztak létre.

b) Zónák kialakításának biztonsági kritériumai:

- Alap védelemmel ellátott helyiségek:
  - Az alap védelemmel ellátott helyiségekben külön rendelkezés hiányában csak az épületre vonatkozó tűz- és munkavédelmi Szabályzatokban foglaltakat kell alkalmazni.
  - A portás feladatokat ellátó személy fő szabályként csak vizuális ellenőrzést gyakorol, a szokatlan vagy veszélyes események megfigyelése vagy intézkedés céljából

- A fokozott védelemmel ellátott helyiségeket az alap védelmen felül:

  - a portán elhelyezett proximity belépőkártyás rendszerrel látta el a Hivatal, belépésre csak az arra jogosult személyek kapnak belépési jogosultságot, az azonosítása személyre szabott, egyedi Proximity kártya használatával történik, a belépéseket a biztonsági rendszer naplózza,
  - fokozott védelem része, hogy a Hivatal egyes ingatlanrészein külön ajtó beléptető és kártya alkalmazását írja elő.

- Kiemelt védelemmel ellátott helyiségek

  - folyamatos folyosói kamera rögzítés lehetséges olyan folyosón vagy helyiségben, ahol nem történik közvetlen munkavégzés,
  - időszakos mozgásérzékelő van működésben,
  - informatikai célú helyiség esetén helyiségen belüli kamera működtetése, páratartalom mérés, tűzérzékelés, önműködő tűzelfojtás, portai vészlekapcsoló,
  - a bejárati ajtóinak automatikus záródását tilos megakadályozni; az automatikus ajtó behúzó szerkezet hiánya esetén gondoskodni kell arról, hogy az ajtó ne maradjon nyitva, illetve ne maradjon illetéktelenül nyitható állapotban;

A zónákba történő be- és kilépést a beléptető rendszer elektronikusan naplózza. A beléptetőrendszer által rögzített adatok: az intelligens kártya azonosítója, belépés és kilépés időpontja, kártya leolvasásának helye, kártyabirtokos neve.

Az adatkezelés időtartama: a Hivatal az Szvtv. 32. § (2) és (3) bekezdése alapján:

- rendszeres belépés esetén: a működtetéshez kezelt adatokat a jogosultság megszűnéséig, a működtetés során rögzített adatokat a jogosultság megszűnésekor, de legfeljebb 6 hónapig,
- alkalmi belépés esetén 24 óráig tárolja az adatokat, ezt követően törli őket.

Az elektronikus beléptető rendszer személyes adat adatkezelői továbbítása: a Hivatal a beléptetésről készíthető naplózási riportokat nem továbbítja (kivéve: bűncselekmény vagy szabálysértés gyanúja, illetve

hatósági megkeresés esetén az illetékes hatóságnak).

30. Kamerás megfigyelő rendszer

Egyes helyiségekben mozgást érzékelő kamerás megfigyelő és ellenőrző rendszer működik.

a) A kezelt személyes adat: élő, valós idejű monitorkép és az érintettekről digitális jelként rögzített képfelvételek.

b) **A kamera időazonos megfigyelésének és az adatrögzítés céljai:**
- a személy- és vagyonvédelem, valamint épület védelem biztosítása,
- az információbiztonsággal kapcsolatos jogszabályi kötelezettségek teljesítése,
- a személyes adatokkal kapcsolatos adatvédelmi incidens kivédése érdekében a jogsértések megelőzése, észlelése, az elkövető tettenérése,
- a jogsértések bizonyítása, és
- az előforduló esetleges balesetek, természeti jelenség okozta károk körülményeinek a dokumentálása.

c) A személyes adatokhoz való adatkezelői hozzáférés. Az élő és a rögzített képet a Hivatal erre vonatkozó rendszerhasználati jogosultsággal bíró informatikus kollégái, valamint az eljárástól függően a Hivatal által megbízott információ biztonságért felelős személy és / vagy a Hivatal jogi képviselője kezel(het)ik. A hozzáférési jogosultságokat a Jegyző engedélyezi a nevezett személyeknek.

d) A személyes adat adatkezelői továbbítása: a Hivatal kizárólag olyan külső szervezeteknek adja át a tárolt felvételeket, akik igazolják adatkezelésük jogszerűségét. Így például a bűnüldöző szervezetek, a bíróságok megkeresése esetén a tényállás tisztázása érdekében az adatok átadására vagyunk kötelesek.

e) Az adatkezelés időtartama: a Hivatal a rögzítéstől számított legfeljebb három munkanapig tárolja a felvételeket, ezt követően az adatokat rotációs rendszerben törli.

31. Hőmérséklet és páratartalom ellenőrzés. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem.

a) Egyes kiemelt védelemmel ellátott helyiségekben az erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet és páratartalmat. Az üzemi hőmérséklet 18, a helyiség hőmérsékletének 24 °C fölé emelkedése esetén a felügyeleti eszköz riasztást küld az üzemeltető számára.

b) A szerver eszközöket is tartalmazó kiemelt védelmű helyiségekben, adatközpontokban redundáns kialakítású klímaberendezést kell üzemeltetni. A redundáns kialakítás történhet nem a helyszínen tárolt mobil-klíma berendezés használatával is, amennyiben az a riasztást követő 1 órán belül a helyszínre szállítható.

c) Egyes helyiségeket a Hivatal védi a víz-, és más, csővezetéken szállított anyag okozta kár ellen. A kiemelt védelemmel ellátott helyiségek kialakításánál törekedni kell arra, hogy a helyiségek távol kerüljenek a víz- és más ilyen módon szállított csővezetékeitől.

d) Az épületek üzemeltetéséért felelős biztosítja, hogy a főelzárószelepek hozzáférhetőek, és

megfelelően működnek, valamint a kulcsszemélyek számára ismertek, valamint, hogy az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. adatközpont, szerver szoba, központi gépterem) során a helyiségek víz-, és más hasonló kártól védettek legyenek, akár csővezetékek kiváltásával, áthelyezésével is.

32. Áramellátás biztosítása

A Hivatal a szerverek, adatátviteli eszközök és más informatikai szempontból kritikus hálózati, biztonsági vagy egyéb eszközei számára az épület kábelezésétől független áramellátó rendszert üzemeltet.

Az áramellátó rendszerben található kapcsolók, kismegszakítók, biztosítékok és érintésvédelmi kapcsolók a kiemelt védelemmel ellátott helyiségekben, kulccsal zárható, védőfölddel ellátott fém szekrényekben kerülnek kialakításra.

33. Tűzvédelem

a) A Hivatalban kialakított tűzvédelmi eljárásrendet a Tűzvédelmi Szabályzat tartalmazza.

b) Az informatikai helyiségek kialakításánál törekedni kell arra, hogy a padlóburkolatok, berendezési tárgyak tűzálló és antisztatikus anyagból legyenek.

c) A kiemelt védelemmel ellátott helyiségekben ügyelni kell arra, hogy a nyílászárók tűzbiztos kialakításúak legyenek, a helyiségekben független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezések kerüljenek kialakításra és karbantartásra.

d) A tartalék helyszínen és az egyéb, személyzet által folyamatosan nem felügyelt elektronikus információs rendszerek számára automatikus tűzelfojtási képességet kell biztosítani.

e) Az elektronikus információs rendszer védelmére szolgáló tűzjelző berendezés vagy rendszert tűz esetén automatikusan működésbe lép, és értesítést küld az érintett szervezet által kijelölt tűzvédelmi felelősnek.

34. Vészkikapcsolás.

a) Az informatikai eszközök működtetésére kialakított áramellátó rendszer a Hivatal portaszolgálatánál tűzvédelmi főkapcsolóval rendelkezik. A tűzvédelmi főkapcsoló áramtalanítja a független informatikai áramellátó hálózatot is.

b) A vészkikapcsolást a portaszolgálat felügyeli és ellenőrzi, gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről, valamint megakadályozza a jogosulatlan vészkikapcsolást. Vészhelyzetben a vészkikapcsoló használatával elvégzi a szükséges áramtalanításokat.

35. Tartalék áramellátás

a) A Hivatal a központi eszközeinél, elsősorban az informatikai helyiségben működő Központi rendszereihez, valamint a kiemelt fontosságú munkaállomásokhoz szünetmentes áramellátást biztosít arra az időszakra, amíg a vélhetően tartós áramkimaradás esetére az informatikai eszközöket

szabályosan le lehet állítani.

b) Megfelelő mennyiségű és kapacitású szünetmentes áramforrással rendelkezik a Hivatal, legalább olyan kapacitásúval, hogy rövid ideig tartó kimaradás esetén az eszközök biztonságosan tovább működjenek, tartós kimaradás esetén az eszközöket biztonságosan le lehessen állítani, így a különösen magas anyagi kár kiszűrhető.

c) A szünetmentes tápellátásnak legalább 30 percig biztosítania kell a szerverek számára az áramellátást, legalább 20 percig tartó áramkimaradást követően a szervereket biztonságosan le kell állítani.

d) A szünetmentes áramellátás UPS tápegység üzemeltetésével valósul meg. A Informatikusok évente kötelesek a szünetmentes tápellátás rendelkezésre állását tesztelni, szükség esetén gondoskodik az akkumulátorok vagy a hibás eszközök cseréjéről, javításáról, karbantartásáról.

36. Vészvilágítás

a) Az informatikai helyiségek kialakításánál gondoskodni kell automatikus vészvilágítási rendszert kiépítéséről és karbantartásáról, amely rendszer áramszünet esetén aktiválódik, és biztosítja a vészkijáratokat és a menekülési útvonalakat.

b) Áramkimaradás esetére intelligens, címezhető biztonsági és irányfény világítási lámpatestekkel a Hivatal rendelkezik.

37. Hozzáférés az információs rendszerhez, adatátviteli eszközökhöz és csatornákhoz, kimeneti eszközök hozzáférés ellenőrzése.

a) A Hivatal információs rendszereit, adatátviteli eszközeit és átviteli csatornáit fizikai és logikai védelemmel is meg kell óvni az illetéktelen felhasználástól és ezt a Hivatal szervezeti egységek vezetői folyamatosan ellenőrzik.

b) Az ilyen helyiségekbe történő **belépéshez és az eszközökhöz** való hozzáféréshez a létesítménybe történő fizikai belépés ellenőrzésén túl külön engedély kell, amely a fent leírt azonosító eszközök és a hozzájuk tartozó jogosultságok alapján adható.

c) Belső hálózati adatátviteli eszközök védelme. Az adatátviteli eszközöket minden esetben zárható helyiségekben kell tartani. A helyiséget kiemelt védelmű zónának kell nyilvánítani és az ennek megfelelő védelemmel kell ellátni. Amennyiben az adatátviteli eszközöket tartalmazó helyiség nem zárható el az illetéktelenek hozzáférésétől, úgy magát az eszközöket tartalmazó szekrényt kell a kiemelt védelmű zóna kritériumainak megfelelő védelemmel ellátni!

d) Egyéb adatátviteli eszközök védelme. Nem kell kiemelt védelemmel ellátni azokat az adatátviteli eszközöket tartalmazó helyiségeket és szekrényeket, amelyek nem tartalmaznak a belső hálózathoz közvetlen hozzáférést biztosító eszközöket (pl. publikus internet szolgáltatáshoz szükséges eszközök), de ezeket a helyiségeket és szekrényeket is folyamatosan zárva kell tartani, és a kulcsokat a megfelelő informatikai munkatárs által, fokozott védelmi megoldásokkal arányosan kell kezelni.

e) Hálózati végpontok kezelése. Az adatátviteli eszközök a rendező helyiségekben csak a rendeltetésszerű használatra, bejelentett, regisztrált módon használt strukturált hálózati végpontokon kerülhet sor informatikai hálózati szolgáltatásra. Amennyiben az adott végponton megszűnik a szolgáltatási

kötelezettség, az informatikai munkatársaknak haladéktalanul gondoskodni kell a végponton történő szolgáltatás megszüntetéséről.

f) Az adott strukturált hálózati végpontot haladéktalanul ki kell patch-elni az adatátviteli eszközökből. Ugyanígy kell eljárni a rendező helyiségeket összekötő optikai hálózati végpontokkal is. A használaton kívülre helyezett optikai szálak patch-elését mindkét oldalon meg kell szüntetni!

38. Az elektronikus információs rendszer elemeinek elhelyezése

a) Az érintett szervezet úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.
b) Az informatikai helyiségek kialakítása elkülönített, fizikailag jól elhatárolt belső épületrészekben történt meg.

39. Az elektronikus információs rendszerek ellenőrzése és karbantartása.

Az informatikai üzemeltetők és / vagy a Hivatal által a fizikai védelmi rendszerek karbantartásával megbízott vállalkozó:

a) A tűzoltó rendszerre vonatkozóan tervszerű megelőző karbantartást végez;
b) Szükség esetén kiegészíti és / vagy cseréli vagy javítja a meglévő rendszer hibás vagy hiányzó eszközeit, alkatrészeit;
c) Ellátja az akkumulátorok terheléses ellenőrzését;
d) Az eszközök működőképességét ellenőrzi, hatékonyságát növeli, különös tekintettel a kamerák megfelelő optikai irányba állításával;
e) A rendszer rendellenes működést elhárítja, a Megrendelő által megjelölt eszközöket letisztítja, a bekötéseket és sorkapcsolásokat, az akkumulátorok terhelhetőségét, a távjelzések működőképességét ellenőrzi, szükség esetén javítja;
f) A fizikai hozzáférés-védelmi rendszer szoftvereit haladéktalanul frissíti;
g) A firmware (elektronikai eszközök vezérlését szolgáló) programokat haladéktalanul frissíti;
h) A Megrendelő szakemberei részére rövid szakmai tanácsadást végez;
i) Az általa érzékelt eszköz és / vagy program hiba észlelése esetén, valamint a Megrendelő hiba bejelentésének esetén, az attól számított 4 órán belül helyszíni ellenőrzést és karbantartást megkezdi;
j) Havonta ellenőrzi a távjelző berendezéseket;
k) Havonta ellenőrzi a vészlekapcsolókat (EPO: emergency power off) és ennek eredményéről jegyzőkönyvet készít;
l) Havonta 1 alkalommal, legalább 2-2 db tűzjelző érzékelő ellenőrzését és ennek eredményéről jegyzőkönyv készítését elvégzi;
m) Vezeti a saját szerkesztésű Karbantartási napló-t;
n) A megbízott vállalkozó és / vagy alvállalkozója vesz részt a Hivatal képviselője által tartott IT biztonsági oktatáson.
o) A vállalkozó titoktartási kötelezettséget vállal.
p) Eseti jelleggel a vállalkozó szakemberei a Hivatal szakemberei részére külön, helyszíni szakmai konzultációt, oktatást nyújt.

XII. Logikai védelmi intézkedések

Az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem, így a Hivatalban az alábbi logikai védelmi intézkedések megtétele

szükséges.

40. Konfigurációkezelési eljárásrend

a) A Hivatal az alábbiakban megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül jelen Szabályzat kihirdetésével kihirdetettnek minősíti a **Konfigurációkezelési Eljárásrendet, Tervet.**

b) A konfigurációkezelési eljárásrendet jelen Szabályzat felülvizsgálata során, de legalább 2 évente felül kell vizsgálni, szükség esetén a változásokat át kell vezetni.

41. Alapkonfiguráció

a) A Hivatalban alkalmazott elektronikus információs rendszereket úgy kell konfigurálni, hogy azok kizárólag a feladatellátáshoz nélkülözhetetlen funkcionalitással rendelkezzenek és szolgáltatásokat nyújtsák **a legszűkebb funkcionalitás elvén.**
b) A Hivatal informatikai rendszerében működő minden eszköz és rendszer csak az Konfigurációkezelési Eljárásrendben meghatározott alapkonfigurációkkal telepíthető.
c) Ettől eltérni csak indokolt esetben az Informatikai Csoportvezető engedélyével lehet.
d) A telepítést kizárólag az informatikai ügyintézők végezhetik a munkaköri leírásukban meghatározott rendszerek, illetve kliens számítógépek vonatkozásában.
e) Az illetéktelen ügyintézői hozzáféréseket jogosítási rendszer alkalmazásával meg kell akadályozni.

42. Az alapkonfiguráció dokumentálása

A Hivatal a szerverekre és a kliensekre vonatkozóan meghatározza az alapkonfigurációk összetételét, verzióit úgy, hogy az alapkonfigurációk csak a munkavégzéshez feltétlen szükséges minimális funkcionalitással rendelkezzenek. Az alapkonfiguráció részletes leírását az **Infrastruktúra Terv Dokumentum** tartalmazza. Az Infrastruktúra tervet folyamatosan karban kell tartani. Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni.

43. A magas kockázatú területek konfigurálása

Az alapkonfiguráció meghatározásakor meg kell különböztetni azt a biztonsági szempontból kiemelten kezelt, alkalmazandó konfigurációt, amely **a külső helyszínen munkát végző hivatali ügyintézők által használt informatikai eszközökre, a hivatali rendszer külső használatára vagy a belső hálózaton használandó külső eszközökre vonatkozik.**

44. Konfiguráció telepítés

a) A Hivatal informatikai rendszerében működő minden eszköz és rendszer csak az **Infrastruktúra Tervben meghatározott alapkonfigurációkkal telepíthető!** Ettől eltérni csak nagyon indokolt esetben az Üzemeltetési és Informatikai Csoportvezető engedélyével lehet!
b) A telepítést kizárólag az informatikai ügyintézők végezhetik a munkaköri leírásukban meghatározott rendszerek, illetve kliens számítógépek vonatkozásában. Az illetéktelen ügyintézői hozzáféréseket jogosítási rendszer alkalmazásával meg kell akadályozni.

45. Változáskezelés, változáskövetés

A Hivatal az alábbiak szerint meghatározza a változáskezelési típusokat.

- Az alapkonfiguráció változása

  - Az alapkonfigurációk változása (új vagy változott rendszerelemek telepítése, beállítások módosítása, hibajavítások kizárólag a belső szabályozásokkal és eljárásokkal egyeztetve történhet.

  - Változtatás esetén a kijelölt informatikai ügyintéző az **Infrastruktúra Terv Dokumentációban** átvezeti az Üzemeltetési és Informatikai Csoportvezető által jóváhagyott változásokat verziózottan, majd minden verzió – 2 példányban - az Informatika–páncélszekrényeiben elzártan tárolásra kerül, egyidejűleg gondoskodni kell **a korábbi alapkonfiguráció mentéséről és visszaállíthatóságának** biztosításáról.

  - Ezt követően az új alapkonfigurációt és annak dokumentációját minden hivatali informatikai ügyintéző rendelkezésére kell bocsátani, akik kötelesek a munkaköri leírásukban szereplő rendszerek és szervezeti egységek vonatkozásában gondoskodni a módosítások telepítéséről minden érintett rendszer vonatkozásában.

  - Az Üzemeltetési és Informatikai Csoportvezető, amennyiben szükséges, **auditálja és felülvizsgálja** a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

- **Jogszabály módosítás, vagy egyedi programfejlesztési igények, illetve hibajavítás okán esedékes változáskezelési eljárás menete:**

  - Irodai igény esetén az adott szakiroda vezetője részletes dokumentáció benyújtásával (amely tartalmazza az érintett adatokat, jogosultságokat, adatkapcsolatokat) jelzi a programfejlesztési vagy módosítási, illetve a hibajavítási igényét az Üzemeltetési és Informatikai Csoportvezető felé.

  - Az igényeket minden év elején január 31. napig kell bejelenteni, **év közbeni igény vagy jogszabályváltozás esetén a módosítás hatálybalépését megelőzően legalább 90 nappal,** de legkésőbb a jogszabály megjelenésekor.

  - Az Üzemeltetési és Informatikai Csoport vezetője az érintett irodavezetővel és a felelős üzemeltetővel a fejlesztési igényeket, javításokat adatvédelmi, integritási, sérülékenységi szempontból, valamint a lehetséges kockázatok felmérése, mértékük és bekövetkezésük valószínűségének becslése alapján pénzügyi **forrás és hatásvizsgálatot készít.**

  - A jóváhagyott igényeket priorizáltan a fejlesztő számára átküldi, aki csak a jóváhagyott fejlesztéseket és javításokat a keretszerződésben foglaltak alapján végigvezeti a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során.

  - A fejlesztő a változásokat és ezek lehetséges biztonsági hatásait dokumentálja, kezeli és ellenőrzi, biztosítja ezek sértetlenségét.

  - Az elkészült fejlesztést a fejlesztő felhasználói és üzemeltetői oktatást követően fizikai és logikai rendszerterv, rendszerbiztonsági terv, fejlesztői teszt jegyzőkönyvek csatolásával, verziózott formában **az Informatikusok rendelkezésére bocsátja, aki a dokumentációkat megvizsgálja,** pozitív

elbírálást követően minden verzió dokumentációját lefűzi, a módosításokat a teszt rendszerbe feltölti.

- A feltöltést mind a teszt mind az éles üzemi rendszerben csak a Hivatal feljogosított informatikai ügyintézője és a fejlesztő közösen végezheti, ezt fizikai és logikai **hozzáférés védelemmel is biztosítani kell. Az alkalmazott szerződésekben a szolgáltató erre vonatkozó kötelezettséget vállal.**

- A feltöltéssel egyidejűleg az Intranetes portálon és az integrált rendszer üzenőfalán, valamint a teszt rendszer üzenőfalán is a módosításokról tájékoztatást nyújt. Egyidejűleg közvetlen tájékoztatással is (telefonhívás, e-mail küldés) felhívja az adott szakiroda figyelmét a feltöltött módosításokra. A szakiroda az elkülönített teszt rendszerben a módosításokat teszteli, jegyzőkönyvben rögzíti a teszt eredményeit. Hibamentes teszt esetén értesíti az Informatikusokat a fejlesztés áttölthetőségéről. Az Informatikus ilyenkor a fejlesztést a fejlesztővel közösen az éles rendszerre telepíti.

- Hiba esetén a hiba teljes körű dokumentálásával, reprodukálhatóságának vizsgálatával a szakiroda jegyzőkönyvet vesz fel, amelyet az Informatikai Csoportvezető számára megküld. Az Üzemeltetési és Informatikai Csoportvezető haladéktalanul értesíti a fejlesztőt a hibáról a jegyzőkönyv másolatának megküldésével. A fejlesztő a hibát javítja, majd a javított fejlesztéssel a fenti eljárásrendet mindaddig ismételni kell, amíg a minden tesztesetre kiterjedő helyes működés be nem következik.

- Hibajavítás esetén, ha a hiba kisebb volumenű, egyértelmű, és a javítást követően láthatóan nincs szükség tesztelésre, a javítás az éles rendszeren (ún. hotfix módon) is elvégezhető. Ezt a fejlesztő az Üzemeltetési és Informatikai Csoportvezetővel történt konzultációját követően az Üzemeltetési és Informatikai Csoportvezető engedélyével telepítheti az éles rendszerre.

- A teszt vagy oktatási rendszeren teszteléskor észrevett hibák hasonlóan javíthatók a teszt vagy oktatási rendszeren, ehhez az Üzemeltetési és Informatikai Csoportvezető külön engedélye nem szükséges.

- Több irodát érintő változáskezelési eljárást az érintett szakirodák vezetőinek egyetértésével, a Jegyző engedélyével a fenti eljárásmód szerint kell végezni.

- Minden éles üzemi rendszert érintő telepítést megelőzően teljes, az alkalmazásokra is kiterjedő mentést kell végezni.

- **Az integrált informatikai rendszer változáskezelés esetén a tesztelés, képzés és felügyelet**

  - Hivatal az új vagy jogszabályváltozás vagy hibajavítás okán módosított elektronikus információs rendszerrel kapcsolatban a fejlesztőtől az üzemeltetők, kiemelt felhasználók és végfelhasználók számára tesztelési és oktatási és felügyeleti lehetőséget kér szerződéses kritériumként.

  - A szerződésben definiálni kell vagy a vállalkozóval, fejlesztővel tudomásul kell vetetni a fenti eljárásrendet, lehetőséget kell teremteni annak fejlesztésére és fenntartására, biztosítani kell a folyamatos időbeni végrehajtását. A fenti eljárásrendet jelen Szabályzat felülvizsgálatával egyidejűleg felül kell vizsgálni, a kockázatelemzési és kezelési terv, valamint a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.

- **Külső szolgáltatótól igénybe vett szolgáltatás változáskezelése**

- A külső szolgáltatókkal kapcsolatos változáskezelés eljárásrendje azonos a Változáskezelési eljárásrenddel, azzal a különbséggel, hogy a részlet szabályokat az üzemeltetővel kötött szerződésben definiálni kell. A teszt rendszert és a biztonsági mentést a szolgáltató biztosítja.

- Új szolgáltatás beszerzése esetén a fenti eljárásrend szerződéses kötelemként történő megfogalmazása kötelező.

- Mindennemű változást úgy kell igényelni, hogy annak a biztonsági kockázatait időben fel lehessen mérni, a szükséges változásokat időben, biztonságosan el lehessen végezni. Új dolgozó számára történő infrastruktúra és jogosultság biztosítása érdekében legalább a munkába állást megelőző 5 munkanappal, a jelenlegi struktúrában történő változás (költözés, igénylés, jogosultság visszavonása) esetén a változást megelőző legalább 3 munkanappal korábban írásban jelezni kell az igényeket.

- A Hivatalban alkalmazott elektronikus információs rendszerek között létesítendő belső rendszer kapcsolatokat az összekapcsolást megelőzően a kockázatelemzési és kezelési tervben szereplő eljárásrend szerint fel kell mérni. Amennyiben az összekapcsolás arányos védelmi intézkedések alapján elvégezhető és az elektronikus információs rendszerek biztonsági osztályba sorolását nem befolyásolja, Jegyző engedélyével végezhető.

- A belső kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát **az Infrastruktúra tervben definiálni kell.**

46. Alkalmazható szoftverek meghatározása

A Hivatalban mind a szerver, mind a kliens oldali eszközökön használható szoftverek jegyzéke az **Alkalmazáskatalógus** dokumentumban kerül részletezésre.

a) A Hivatal a futtatható és a nem futtatható szoftverek vonatkozásában csak a telepíthető szoftverek jegyzékét határozza meg, **ún. fehér listás (white-list) eljárással.** A telepíthető szoftverek jegyzékét az Alkalmazáskatalógus tartalmazza. Minden az Alkalmazáskatalógusban található fehér listás alkalmazástól eltérő szoftver nem telepíthető és nem futtatható.

b) Telepítések korlátozása.
A kliens oldali rendszerekben a telepítési jogosultság rendszer adminisztrátori joghoz kapcsolódik. Felhasználói joggal a rendszerben semmilyen alkalmazást nem lehet telepíteni! A kliens számítógépeken a felhasználók nem kaphatnak adminisztrátori jogokat!

c) BIOS korlátozása.
A számítógépeken a (BIOS-ban a) rendszerbetöltési prioritást csak merevlemezre szabad korlátozni, semmilyen más eszközről rendszer betöltését engedélyezni nem szabad! A rendszerek BIOS-át jelszavas védelemmel le kell tiltani.

A jelszót csak az informatikai ügyintézők ismerhetik, azt továbbadni nem szabad. A BIOS jelszavakat kompromittálódás esetén ki kell cserélni.

Az új beszerzésű eszközök esetében – hardverkonfigurációnként – mindig új BIOS jelszót kell adni. A BIOS jelszavakat konfigurációk megjelölésével lezárt borítékban az Informatikai Csoportnál elhelyezett a fő és a tartalék helyszíneken zárt páncélszekrényekben kell tartani.

d) Változáskezelés.
Amennyiben a Hivatal rendes működéséhez elengedhetetlen új szoftverek használata, úgy az az Alkalmazáskatalógusban a megfelelő, jelen Szabályzatban meghatározott változáskezelési eljárásrendet követően átvezetésre kerül.

47. A szoftverhasználat korlátozásai.

a) Nyílt forráskódú, szabad szoftverek.
A Hivatal minden olyan munkaállomáson, ahol nem veszélyezteti a feladatellátást, a közös üzemeltetésű feladatokat, az ASP rendszer működtetését, az e-közigazgatási feladatok ellátását, ott kizárólag nyílt forráskódú és/vagy szabad szoftvereket (FLOSS) telepít.

Mivel ezeknek a szoftvereknek nincs egyedi azonosítója, ezek nyilvántartása csak megnevezés alapján, az adott leltári azonosítójú eszköz azonosításával összerendelve történik. A telepíthető szoftverek listáját az Alkalmazáskatalógus dokumentum tartalmazza.

b) Licence-elt szoftverek.
Azokon a munkaállomásokon, ahol a feladatellátás megköveteli a zárt kódú, ún. licence-elt szoftvertermékek futtatását, ott a változáskezelési eljárásrend szerint megigényelt és jóváhagyott engedély alapján történik a szoftvertermékek beszerzése.

c) OEM rendszerek.
A hardverhez kapcsolt szoftver licencek: az ún. OEM licencelt rendszerek és alkalmazások licence-e a hozzá tartozó hardverrel együtt kerül regisztrálásra a leltár szoftverben. A szoftverlicence azonosító matricája a hardverre kerül felragasztásra.

d) Mennyiségi licencek.

A mennyiségi vagy szabad felhasználású licence-k az Informatikai Csoport páncélszekrényében kerülnek tárolásra. A licencekhez bontható kötéssel hozzá kell kapcsolni az igénylő dokumentumot (anélkül, hogy a licence megsérülne), amelyen fel kell tüntetni, hogy az adott licence melyik felhasználó melyik eszközére került telepítésre.

A szoftverlicence-k csak akkor telepíthetők másik gépre, ha az előző gépről eltávolításra kerültek, és ezt a szoftverlicencek mellé csatolt dokumentumban is átvezetésre került.

Tilos egy licencet több gépre is telepíteni, ha ezt a szoftver licencpolitikája nem engedi!

e) Egyéb szoftverek.

Tilos a Hivatal informatikai eszközeire olyan szoftverterméket telepíteni, amelyhez a Hivatal nem rendelkezik megfelelő szoftverlicence-el.

Tilos továbbá olyan szoftvertermék telepítése, amely feltörésre került, vagy a másolását/felhasználását korlátozó védelmi intézkedés kikerülésre került.

Nem használható továbbá shareware, demo és egyéb olyan szoftvertermék, amelynek közületi felhasználása nincs korlátlanul engedélyezve.

Nem telepíthető olyan szoftvertermék sem a számítógépekre, amelyekhez a Hivatal nem, de a felhasználó rendelkezik hozzáférési vagy telepítési joggal!

f) Hordozható informatikai eszközök telepítése.

a) A személyi leltárba adott informatikai eszközök és/vagy hordozható eszközök **átadás-átvételi** jegyzőkönyvére rá kell vezetni az eszközre telepített operációs rendszer megnevezését, verziószámát, amennyiben licence-elt rendszert tartalmaz, a felhasználói licence számát és azonosítóját (kulcsát) valamint a telepített szoftverek listáját és amennyiben ezek között licence-köteles termék is telepítésre került, úgy a felhasználói licenc azonosítóját, azonosítóit.

b) A jegyzőkönyvben ki kell kötni, hogy a telepített szoftverek és komponensek önkényes megváltoztatásáért az átvevő teljes körű anyagi és erkölcsi felelősséget vállal, az adatok mentése a használó feladata.

g) Mobil kódok korlátozása.

a) A Hivatali infrastruktúrában kizárólag a Alkalmazáskatalógusban meghatározott alkalmazásokkal szabad mobil kódokat futtatni. Tilos olyan mobil kódokat futtatni, amelyek futtatásához szükséges szoftvertermék nem szerepel a Alkalmazáskatalógusban.

b) Amennyiben mégis ilyen kód futtatása szükséges, úgy azt az Alkalmazáskatalógusban történő változáskezelési eljárást követően igényelhető.

c) A mobil kódok futtatása minden esetben az Informatika előzetes biztonsági vizsgálata alapján történhet, az Információbiztonságért felelős személy döntése alapján; ennek hiányában mobil kódokat futtatni tilos!

48. Elektronikus információs rendszerelem leltár

a) **Számviteli leltár** A Hivatal az elektronikus rendszerelemei nyilvántartásához és leltározásához a számviteli leltár programot használja.

b) Az eszközök beszerzésekor a beszerzett eszközök számviteli nyilvántartásba kerülnek. Az eszközök beszerzésekor, változásakor selejtezésekor a nyilvántartó rendszerben a változások átvezetésre kerülnek.

c) A Hivatal a Szabályzat alapján gondoskodik arról, hogy a leltár:
- pontosan tükrözze az elektronikus információs rendszer aktuális állapotát
- az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza;
- legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.
- az egyes rendszerelemek telepítésének, eltávolításának, frissítésének időpontjában a leltár is kerüljön frissítésre.
- az Infrastruktúra Terv és a leltár legyen összhangban.

49. Nyilvántartás duplikálás elleni védelem

a) Az elektronikus információs rendszerelemek a számviteli és az Üzemeltetési és Informatikai Csoport

saját nyilvántartásában szerepelnek.

b) Más rendszerelem leltárba csak akkor vihetők fel, ha a két (vagy több) nyilvántartó rendszer között reláció hozható létre, vagy manuálisan össze lehet rendelni (pl. azonosító szám alapján) az elektronikus rendszerelemek nyilvántartását.

c) Több nyilvántartás vezetése és a fentiek nem teljesülése esetén a Hivatal ellenőrzi, hogy az elektronikus információs rendszer hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárába.

50. Rendszerelem leltár naplózása

a) Az elektronikus információs rendszerelem számviteli leltár esetén a Leltározási Szabályzatban meghatározottak szerint az egyes elemek adminisztrálásáért felelős személyek nevét, pozícióját vagy szerepkörét meg kell jeleníteni.

b) Az elektronikus információs rendszerelemek Informatikai Csoport saját nyilvántartásáról rendszeresen papír alapú kivonatot kell készíteni, amelyet az egyes elemek adminisztrálásáért felelős személyek nevét, pozícióját vagy szerepkörét meg kell jeleníteni, és a kivonatot az Informatikai páncélszekrényben kell elhelyezni.

51. Személybiztonsági, azonosítási, hitelesítési, hozzáférési eljárásrend

a) **Felelősségi körök szétválasztása** Hivatalban a munkakörök és felelősségi körök dokumentáltan – a munkaköri leírások alapján – szétválasztása kerülnek, ami meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

b) **Egyedi azonosítás, jogok.** A Hivatal biztosítja, hogy minden munkatársa megfelelő, egyedi és azonosítható hozzáféréssel rendelkezzen a munkaköréhez szükséges a munkaköri leírásában szereplő feladatok ellátásához kapcsolódó informatikai alapszolgáltatásokhoz és személyes vagy csoportos felhasználói fiókjához.

c) **A Hivatal minden munkatársa** számára biztosítja a munkakör ellátásához szükséges felhasználói alkalmazások, illetve a felhasználói alkalmazások meghatározott részeinek rendeltetésszerű használatát megfelelő azonosítási és hitelesítési eljárást követően.

d) **Munkakörhöz kapcsolódó jogok. A Hivatalban** az elektronikus információs rendszerekhez és fiókokhoz kiosztott jogosultságok munkaköri besoroláson alapulnak, ugyanabban a munkakörben dolgozó munkatársak ugyanolyan jogosultságokkal rendelkeznek. Ettől eltérni csak egyedi esetekben, az adott szakiroda vezetője és az Üzemeltetési és Informatikai Csoportvezető engedélyével, dokumentáltan lehetséges.

52. A legkisebb jogosultság elve

a) Az informatikai jogosultságokat úgy kell engedélyezni, hogy a felhasználó minden, a munkájához szükséges, és csak a szükséges adatokhoz és alkalmazásokhoz a megfelelő legszűkebb mértékig férjen hozzá.

b) Bármilyen **adathordozó használata a végfelhasználók számára tilos.** Ettől eltérni csak a jelen Szabályzatban meghatározott feltételek teljesülése esetén szabad.

c) Azon felhasználók, akik eltérő rendszerekhez is jogosultsággal rendelkezhetnek és a munkakörük alapján kötelesek külső harmadik személytől adathordozót átvenni; különös tekintettel a pályázatok, közbeszerzési ajánlatok, műszaki tartalmú dokumentációk mobil adathordozón történő átvételi kötelezettségére, az Informatikai biztonságért felelős személy részére kötelesek írásban bejelenteni az adathordozó átvételt.

d) A Hivatal megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

53. A Hivatal elektronikus információs rendszereihez történő informatikai jogosultságok kiadása

a) Minden új belépő és / vagy új munkakört ellátó munkatárs a személyazonosítását követően a Személyzeti dolgozók által kiállított igazolás, valamint a szakiroda vezetőjének javaslata és a munkaköri leírásában szereplő feladatok alapján a munkaköréhez szükséges adatokhoz, alkalmazásokhoz hozzáférést kap.

b) A középvezető köteles legalább az informatikai jogosultságok gyakorlását **megelőző 3 munkanappal** korábban e-mail-en keresztül a jogosultságot megigényelni az Informatikusoktól.

c) A középvezető köteles legalább az informatikai jogosultságok gyakorlását **megelőző 3 munkanappal** korábban keresztül azt is jelezni, ha a munkavállaló tartós távolléti státuszból tér vissza és korábban felhasználói informatikai jogosultsággal rendelkezett.

d) A szakiroda illetékességén túlmutató jogosultságok kizárólag a szervezeti egység vezetőjének kérésére, a Jegyző jóváhagyásával állítható be.

e) Az azonosítók kiadásakor ellenőrizni kell, hogy a kiadni kívánt azonosító korábban kiadásra került-e a rendszerben. Nem adható ki olyan azonosító, amely korábban már más személyt azonosított az adott elektronikus információs rendszerben.

54. Az elektronikus információs rendszerekhez történő informatikai jogosultságok megszüntetése, a személyes adatok törlése.

a) A felhasználó foglalkoztatási jogviszonyának megszűnése esetén, a iroda vagy csoportvezető köteles minél korábban, de legalább a jogviszony megszűnését **megelőző 3 munkanappal** korábban a jogosultságok megszüntetését kérni. Emellett a felhasználó a Személyzeti dolgozók által kiállított ún. „sétálólappal" tudja igazolni a megszűnéssel kapcsolatos teendőinek az ellátását, különösen informatikai eszköz leadása, a dokumentumok hálózati könyvtárba való mentése.

b) A szervezeti egység vezetőjének nyilatkoznia kell, hogy a felhasználó jogviszonyának megszűnéséig melyik más, aktív felhasználó levelezési fiókjába kerüljön átirányításra az addig lezajló levelezési tartalom

c) Amennyiben az érintett felhasználó külső rendszerekhez is kapott hozzáférést, a külső rendszer kapcsolattartója köteles a külső szolgáltatót haladéktalanul értesíteni a jogosultság megszűnésének

tényéről.

d) A felhasználó foglalkoztatási jogviszonyának megszűnésével egy időben az érintett felhasználó levelezési fiókjának tartalmát az üzemeltető törölni köteles, kivéve, ha az érintett felhasználó másképp rendelkezik írásban.

e) Az informatikai üzemeltető köteles a felhasználóhoz tartozó összes hozzáférési jogosultságot (a hivatali ügyfélkapu jogosultságot is) haladék nélkül a jogviszony megszűnésének napjáig bezárólag **megszüntetni, és / vagy visszavenni** a személy egyéni hitelesítő eszközeit vagy használatra kiadott, az elektronikus információs rendszerrel kapcsolatos, a Hivatal tulajdonát képező összes eszközt.

f) Mivel a hivatali számítógépeken és informatikai eszközökön magáncélú adatok tárolása tilos, így az adatok kimásolására nincs mód.

g)

h) Amennyiben a felhasználó külső rendszerekhez is kapott hozzáférést, a külső rendszer irodai kapcsolattartója köteles a külső szolgáltatót haladéktalanul értesíteni a jogosultság megszűnésének tényéről.

i) **A külső rendszerek fiókkezelőit** akkor is értesíteni kell, ha egy adott felhasználói fiókra már nincs szükség, a felhasználó kilépett vagy áthelyezésre került, valamint, ha az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak.

j) A felhasználó az olyan szakrendszerekből, amelyekben a nevéhez köthető, hivatalos cselekmény történt, és archiválásra került, a felhasználó nem törölhető, csak a státusza **„inaktívvá" tehető.** Az ilyen szakrendszerekből a kilépő személyhez kapcsolódó dokumentumok az Iratkezelési Szabályzat és az **ágazati jogszabályok** által előírt tárolási időn belül nem törölhetők.

k) A jogviszonyt megszüntető személy köteles az elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodni, az elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzni.

55. Az informatikai jogosultságok módosítása

a) A felhasználó munkatárs informatikai jogosultságainak bővítése, szűkítése az illetékes szervezeti egység vezetőjének kezdeményezésére történhet, legalább az informatikai jogosultságok gyakorlását **megelőző 3 munkanappal** korábban.

b) Meg kell különböztetni, hogy a bővítés vagy szűkítés csak egy adott munkatársat, vagy minden, adott munkakörben dolgozó munkatársat érint-e, és szükség esetén a munkakörökhöz tartozó jogosultsági listát is módosítani kell.

56. Munkaköri áthelyezés esetén az informatikai jogosultságok módosítása

a) A felhasználó más munkakörbe történő áthelyezésekor az informatikai jogosultságainak bővítése, szűkítése az illetékes szervezeti egység vezetőjének kezdeményezésére, továbbá az új szervezeti egység vezetőjének jóváhagyó bejelentésével történhet, legalább az informatikai jogosultságok gyakorlását **megelőző 3 munkanappal** korábban.

b) Ettől eltérni csak a Jegyző írásbeli kérésére lehet.

c) Az informatikai üzemeltetők nem adhatnak ki új szakirodai jogosultságot addig, amíg a korábbi jogosultságok nem kerültek megszüntetésre.

57. Munkaköri tartós távollét

a) A munkavállaló tartós távolléte vagy egy hónapot meghaladó távolléti időtartam esetén, az illetékes középvezető köteles minél korábban, de legalább a tartós távollét **bekövetkezte utáni 3 munkanapon belül** a jogosultságok felfüggesztését, megszüntetését kérni.

b) Az illető felhasználó munkatárs jogosultságait a távollét időtartamára teljes körűen fel kell függeszteni.

58. Azonosítási-hitelesítési és személybiztonsági eljárásrend.

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti minden felhasználóját, és az általuk végzett tevékenységeket.

59. A hitelesítésre szolgáló eszközök kezelése, azonosítása és hitelesítése

a) A hitelesítésre szolgáló eszközöket egyedi azonosítójuk szerint névre szólóan nyilván kell tartani. **Nyilván kell tartani továbbá az eszközökkel kapcsolatos minden történést (átadás-átvétel időpontja, dátuma, kompromittálódás, elveszítés, csere, sérülése, visszavonása, érvényessége, érvénytelensége.**

b) Az eszközök kezelését és nyilvántartását az Üzemeltetési és Informatikai Csoportvezető és / vagy az általa megbízott üzemeltető végzi.

c) **Az eszközöket átadás-átvételi jegyzőkönyvvel csak az eszközt használó számára személyesen lehet kiadni és tőle visszavételezni.** A személyek azonosságát és jogosultságát minden esetben ellenőrizni kell!

d) A jegyzőkönyvben rögzíteni kell a hitelesítésre szolgáló eszközök azonosítóját, az átadás átvétel dátumát, pontos időpontját, az átadás-átvételben részt vevő személyeket, a eszközzel kapcsolatos információkat (pl. érvényesség) és védelmi intézkedéseket (a felhasználó köteles az eszköz bizalmasságát és sértetlenségét minden rendelkezésére álló eszközzel és megoldással védeni), a felhasználhatóság feltételeit, valamint a felelősségek tudomásul vételét, illetve az eszközök elveszítéséből, kompromittálódásából származó károkkal kapcsolatos felelősségeket és költségeket.

e) Az átadást követően biztosítani kell a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat az átvevő részére.

f) A visszavételt követően, valamint az eszköz kompromittálódásának, elvesztésének megismerésekor azonnali hatállyal meg kell szüntetni az eszközhöz kapcsolódó jogosultságokat!

g) A hitelesítésre szolgáló eszközök kezelése során – amennyiben azt a hitelesítésre szolgáló technológia lehetővé teszi:
   - meg kell változtatni a hitelesítésre szolgáló eszköz kezdeti tartalmát
   - meg kell változtatni a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során

- a hitelesítésre szolgáló eszköz típusra, meghatározott időnként meg kell változtatni vagy frissíteni kell a hitelesítésre szolgáló eszközöket
- az érintett fiók megváltozásakor le kell cserélni a hitelesítésre szolgáló eszközt

60. Jelszó (tudás) alapú hitelesítés

a) A Hivatal egyes saját, valamint egyes külső üzemeltetők által működtetett elektronikus információs rendszereihez a belső hálózatból történő hozzáférése egyedi azonosító névvel és a hozzá kapcsolódó jelszóval (tudás alapú hitelesítés során) történik.

b) Felhasználói nevekre vonatkozóan mind a Hivatal, mint a külső üzemeltető kötelező előírásokat fogalmazhat meg a felhasználók és üzemeltetők részére.

c) Jelszavak. A Hivatalban az üzemeltetőknek és a felhasználóknak az információbiztonság folyamatos védelme érdekében törekednie kell az elektronikus információs rendszerekben a jelszavak létrehozása, módosítása során a következő feltételek betartására:

- a megadott jelszó min. 8 karakter hosszú, tartalmazzon legalább 3 számjegyet, és 1 nagybetűt;
- a jelszót legalább 2 hónaponként cserélni kell;
- a megváltoztatott jelszónak legalább 60%-ban különböznie kell a korábbi jelszótól;
- a jelszavak karakteres vagy egyszerűen **visszafejthető módon nem tárolhatók** és továbbíthatók az elektronikus információs rendszerekben;
- a jelszó felhasználónak történő átadása biztonságos módon történjen,
- a kapott jelszót a felhasználónak az első bejelentkezéskor kötelezően meg kell változtatnia,
- a felhasználó köteles titokban tartani jelszavát, és kompromittálódás gyanúja esetén azonnal meg kell változtatnia,
- **adminisztrátori vagy privilegizált fiókokho**z csak személyre (névre) szóló hozzáférés létesíthető, nem lehet általános, nem azonosítható fiókokat (pl. admin.) létrehozni,

61. Visszajátszás (replay) elleni védelem.

a) **Visszajátszás (replay) elleni védelem működik a Hivatalnál, a hitelesítési eljárás** nem játszható vissza egy hálózati csomag elfogásával és későbbi visszaküldésével.

b) Amennyiben a rendszerhez tartozik **mester hozzáférés**, úgy azt lehetőség szerint le kell tiltani, vagy a hozzá tartozó jelszót lezárt, lepecsételt borítékban zárt lemezszekrényben az Informatikai Csoport területén kell tárolni.

62. Birtoklás alapú hitelesítés.

a) A Hivatal a távoli hozzáférésekhez többtényezős, **eszköz alapú hitelesítési eljárást alkalmaz**, ahol az eszköz nem választható el a hitelesítő kulcstól.

b) A Hivatalban a külső hozzáférésekhez alkalmazott eszköz alapú hitelesítési eljárásokat az adott rendszerekkel összefüggésben az **Infrastruktúra Terv tartalmazza.**

c) Nyilvános kulcsú infrastruktúra hitelesítés.

Amennyiben a Hivatalban alkalmazott bármely elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítésen alapul, akkor az alábbi védelmi megoldásokat kell alkalmazni:

- ellenőrizni kell a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;
- ki kell kényszeríteni a megfelelő magánkulcshoz való jogosult hozzáférést;
- össze kell kapcsolni a hitelesített azonosságot az egyéni vagy csoport fiókkal;
- meg kell valósítani a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

63. Tulajdonság alapú hitelesítés.

a) A **biometrikus tulajdonságok** személyekkel összefüggő kezelése, tárolása kizárólag az adatvédelmi szabályok (GDPR, Info tv.) betartásával, a felhasználó beleegyezésével történhet.

b) A biometrikus tulajdonságokat megfelelő titkosítási eljárással kell tárolni, harmadik fél részére kiadni vagy hozzáférhetővé tenni tilos.

c) A Hivatal **nem alkalmaz** biometrikus hitelesítési technológiát.

d) Amennyiben az elektronikus információs rendszerben erre lehetőség van a rendszerben történő hitelesítésre vagy annak biztonsága fokozása érdekében a GDPR előírásainak és a NAIH állásfoglalásának megfelelő érdekmérlegelést kell lefolytatni a biometrikus hitelesítési technológia alkalmazhatóságára.

64. Hivatali Kriptográfiai Útmutató, titkosítási előírások

a) A Hivatal a következő **titkosítási előírásokat** szabja meg a kliensek, felhasználók számára, különösen, ha valószínű a szervezeti adatátadás, adattovábbítás:

- bizalmas adatok kezelése esetén a felhasználó alkalmazza a „keepass" technikai lehetőségeket, tehát a a jelszavai biztonságos tárolását;
- alkalmazza a veracrypt szoftvereket, amelyek könnyen használhatók, nyílt forráskódúak és mindhárom nagy platformra elérhetőek és a segítségével titkosított konténerfájlokat hozhatnak létre és létező partíciókat titkosíthatnak le.
- A feloldó kulcsot a két szintű biztonságnak megfelelően személyesen vagy TELEGRAM-ben kell a kliens részéről eljuttatni az általa megjelölt és biztonságosnak minősített célszervezet képviselőjének. Ezzel bizonyos szempontból mobilitást is kap az alkalmazott biztonsági eljárás.

b) A Hivatal Informatikai szakemberei kötelesek a munkájuk során a következőket betartani:

- a Storage szolgáltatás titkosítás megvalósítása
- a folyamatos mentés titkosítással való ellátása;
- az üzemeltetők és informatikai ügyintézők minden feladat ellátásánál, webes alkalmazások esetén kötelező a „https" használata;
- a beszerzett, de sérült vagy rossz adathordozó az eladónak nem adható vissza, az adathordozó fizikai megsemmisítése kötelező;
- végleges törlés során az üzemeltetők és informatikai ügyintézők Windows rendszer esetén File

shredder - http://www.fileshredder.org/index.php vagy O&O SafeErase professional vagy Ccleaner, Linux-nál killdisk vagy dd if=/dev/zero of=/dev/sdb parancssor alkalmazására kötelesek.

65. A hitelesítésre szolgáló eszköz visszacsatolása

a) Amennyiben az elektronikus információs rendszerhez eszköz alapú hitelesítési eljárás társul, úgy az elektronikus információs rendszerben **fedett visszacsatolást kell biztosítani** a hitelesítési folyamat során, a hitelesítési információk jogosulatlan személyek felfedésétől, felhasználásától történő védelme érdekében.

b) Az elektronikus információs rendszerben alkalmazott kriptográfiai modulokhoz való hitelesítésre kizárólag **az adott kriptográfiai modul hitelesítési útmutatójának** megfelelő technológiákat szabad alkalmazni.

66. Felhasználói fiókok kezelése, eszközök azonosítása és hitelesítése

a) **Felhasználói fiókok kezelésére vonatkozó eljárásrend.**
Hivatalban alkalmazott elektronikus információs rendszerekben jelen Szabályzatban meghatározott eljárásrend szerint kell a felhasználói fiókokat kezelni.

b) **Jogosítási mátrix.**

Az alkalmazáskataszter dokumentumban a jogosítási mátrix alapján minden alkalmazásra meg kell határozni a elektronikus információs rendszer felhasználói fiókjait, azok típusait, meg kell határozni továbbá az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit.

c) **Jogosítások kezelése**

A felhasználói fiókokat az informatikai üzemeltetők kezelik, a munkaköri leírásukban szereplő információs rendszerek és szervezeti egységek vonatkozásában.

A kezelés során az **azonosítás-hitelesítési eljárásrend** szerint a jogosult informatikai ügyintéző létrehozza, engedélyezi, módosítja, letiltja és eltávolítja a felhasználói fiókokat, valamint az eljárásrend szerint folyamatosan ellenőrzi a felhasználói fiókokat.

A jogosítási eljárás során az informatikai ügyintéző az azonosítás-hitelesítési eljárásrend szerint a felhasználókat feljogosítja az elektronikus információs rendszerhez való hozzáférésre az érvényes hozzáférési engedély, a tervezett rendszerhasználat az alapfeladatok és funkcióik alapján.

d) **Jogosítások felülvizsgálata**
A szervezeti egység vezetők, a középvezetők a hozzájuk rendelt informatikai ügyintézőkkel az azonosítás-hitelesítési eljárásrendnél meghatározott gyakorisággal és eljárásrend szerint felülvizsgálják a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot.

e) **Megosztott, csoport fiókok**
Hivatalban nem lehet olyan külső (távoli) hozzáféréssel vagy más okból kialakítani olyan megosztott vagy csoport felhasználói fiókokat, amelyekhez hitelesítő eszközök tartoznak.

f) **Hozzáférés alapvető fiókokhoz**

Minden szervezeti egységben dolgozó felhasználó alapértelmezésben jogosult a szervezeti egységéhez kapcsolódó alapvető fiókhoz és alkalmazásokhoz hozzáférni. További csoport jogokat a felhasználó vezetőjének írásbeli kérésére adható az **azonosítási és hitelesítési eljárásrend** szerint.

67. Hozzáférési csoportok meghatározása.

A Hivatal informatikai rendszereihez az alábbi hozzáférési csoportokat határozza meg:

a) Belső hálózati alapszolgáltatás hozzáférés a Hivatal által meghatározott irodarendszerekhez való hozzáférést biztosítja, ami a belső hálózatra csatlakoztatott minden felhasználói munkaállomáson rendelkezésre áll.
b) Belső hálózati felhasználói alkalmazás hozzáférés a felhasználói alkalmazás használatát biztosítja, ami a felhasználói terület erre jogosult munkatársának a megfelelő **azonosítási és hitelesítési eljárást** követően a munkaállomásán rendelkezésre áll.
c) Felhasználói alkalmazás hozzáférés engedélyezett jogosultság használattal, külső üzemeltető által működtetett elektronikus információs rendszerelemekhez.
d) Belső hálózati privilegizált szolgáltatás hozzáférés a speciális informatikai szolgáltatások (pl. Internet, Laptop használat) igénybe vételét biztosítja.
e) Belső hálózati privilegizált üzemeltetői hozzáférés a Rendszerszoftverekhez (operációs rendszerek) és a rétegszoftverekhez (adatbázis-kezelők) való hozzáférést biztosítja, valamint a felhasználók felhasználói alkalmazásbeli hozzáférési jogosultság beállítását teszi lehetővé. Ilyen jogosultságokkal a kinevezett üzemeltetők rendelkeznek.
f) Külső felhasználói hozzáférés az elektronikus levelezési fiókokhoz.
g) Külső privilegizált hozzáférés a rendszer karbantartásához, ennek során meghatározott módon konfigurált elektronikus információs rendszerelemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják.

68. Ellenőrzési eljárásrend a belső hálózatból történő hozzáférésekhez, jogosultság-kezelési és hozzáférés ellenőrzés.

a) A Jegyző és az Informatikai biztonságért felelős személy az Informatikai munkakörök meghatározását annak megfelelően határozzák meg, hogy az informatikai jogosultságok kezelése pontosan meghatározott személyek által történjen.

b) A rendszer **folyamatos naplózás** ellenőrzésével biztosított az inaktív fiókok kiszűrése és az információáramlás ellenőrzése.

c) A privilegizált jogosultságokról önálló nyilvántartást vezet az Informatikán dolgozó ügyintéző.

69. Nyilvántartások vezetése.

a) Az aktuális Felhasználó neveket és az azokhoz tartozó jogosultságokat az informatikai üzemeltetőknek nyilván kell tartani **(jogosultsági mátrix vezetésével). Azt az informatikai üzemeltetők** a munkaköri leírásban foglaltak szerint vezetik, annak pontosságáért és napra készségéért felelősséggel tartoznak.

b) Az Informatikai biztonságért felelős személy a privilegizált funkciókkal kapcsolatban kötelezővé teszi, hogy az Informatikai munkavállalók a külön jogosultsági mátrixban meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem a **különleges jogosultsághoz kötött - úgynevezett**

privilegizált - fiókjukat vagy szerepkörüket használják.

c) A Hivatal ezzel hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

d) Az erre kötelezettek naplózzák a privilegizált funkciók végrehajtását.

e) A Hivatal elektronikus információs rendszere megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését, vagy megváltoztatását.

f) Az Alapszolgáltatásokkal, felhasználói alkalmazásokkal, és speciális IT szolgáltatásokkal (pl. Internet, Laptop) összefüggő jogosultságok részletes nyilvántartását – melyik felhasználónak milyen jogosultságai vannak – részben űrlapok, részben a felhasználói alkalmazások erre kialakított adatbázisai tartalmazzák.

g) A Felhasználók és üzemeltetők jogosultságainak megváltoztatását előíró, az Üzemeltetési és Informatikai Csoportvezető jóváhagyását tartalmazó leveleket, dokumentumokat az Informatika is nyilvántartja.

70. Tűzfalvédelem és a support szolgáltatása.

A Hivatal információbiztonsága érdekében az Informatikai Csoport munkatársai ellátják a következő feladatokat:

a) a saját logszerver folyamatos monitorozását és üzemeltetését;

b) a szolgáltatásokhoz szükséges szoftverek üzemszerű működésének folyamatos biztosítását;

c) a tűzfalak konfigurációs állományainak napi szintű mentését a Vállalkozó központi management rendszerébe (e rendszer hatékony mentési és katasztrófa elhárítási képességeinek köszönhetően az üzemeltetett rendszer teljes megsemmisülése esetén is rövid időn belül visszaállítható a produktív környezet);

d) a tűzfalak naplófájljainak rendszeres figyelését;

e) a felfedezett, rendellenességekre utaló jelekről jelentés készítését, illetve amennyiben az a rendszeren belüli módosítással megoldható, akkor annak kivitelezését;

f) napi fájlrendszer integritás ellenőrzés;

g) a naplóállományok forgatását, biztonságos archiválását;

h) statisztikák készítését azokon keresztül az adott szolgáltatás ellenőrzését;

i) a biztonsági szoftverfrissítések elvégzését;

j) az időszakosan teljes frissítést (összes szoftver és kernel);

k) online elérés esetén az Internet felől elérhető szolgáltatások, a fájlrendszer-telítettség, a hálózati

interfészek hibái, a futó folyamatok, az entrópia pool, a terhelés (load), a levelező spool-ok telítettsége, a memóriatelítettség, a nyitott fájlok, a belépett felhasználók, a legtöbb memóriát fogyasztók tízes listája, a törölt futtatható állományok folyamatos ellenőrzését;

71. Logikai védelmi intézkedések a jogosultság-kezelés és hozzáférés során.

a) A Hivatal elektronikus információs rendszereiben nem engedélyezett az azonosítás/hitelesítés nélküli tevékenység.

b) **Munkaszakasz zárolása.** Az informatikai üzemeltetők és a felhasználók kötelesek biztosítani, hogy a Hivatalban alkalmazott vagy alkalmazni kívánt elektronikus információs rendszer meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést, valamint megtartja-e a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

c) **Képernyőtakarás.** A munkaszakasz zárolásakor a képernyőn korábban látható információt, egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a záró személy nevét is tartalmazhatja - kell eltakarni.

d) **Munkaszakasz lezárása.** Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

72. A Hivatalban használt informatikai rendszerek használati jogosultságának ellenőrzése

A Hivatalban használt informatikai rendszerek használatának jogosultságát az alábbi eljárásrend szerint folyamatosan ellenőrizni kell.

a) Az Informatikai biztonságért felelős személy közreműködésével, az Informatika munkatársai a szakirodai rendszerek felhasználóinak jogosultságát, a **jogosultsági mátrix-al való egyezőséget folyamatosan, szúrópróba-szerűen ellenőrizhetik,** továbbá a szakiroda vezetője vagy az általa – munkaköri leírásban – e feladatra kijelölt kezdeményezheti.

b) Az ellenőrzés során meg kell állapítani, hogy a vizsgált felhasználó jogosultsága megegyezik-e a munkaköri leírásában szereplő feladatokhoz kapcsolódó jogosultságokkal.

c) Az ellenőrzésről jegyzőkönyv készül, amely tartalmazza az ellenőrzés idejét, helyét, az ellenőrzött rendszert, az ellenőrzésben részt vevő személyek nevét, beosztását, az ellenőrzött jogosultságok felsorolását, az ellenőrzés eredményét, megállapításait.

d) Az elkészült jegyzőkönyvhöz mellékelni kell a vizsgálat tárgyához kapcsolódó rendszerbejegyzést, amelyet a rendszer fejlesztője biztosít, ha az a rendszerből automatikusan nem nyerhető ki.

e) Amennyiben az Informatikai biztonságért felelős személy és / vagy a szervezeti egység vezetője a rendszer biztonsága szempontjából kockázatos rendellenességet tapasztal, haladék nélkül feljegyzés formájában tájékoztatja a Jegyzőt.

f) Az ellenőrzéseket minden felhasználó vonatkozásában a jogosításban bekövetkezett változás esetén

haladéktalanul (azaz az első bejelentkezéskor) ezen felül negyedévente legalább 5 felhasználóra vonatkozóan el kell végezni úgy, hogy a szervezeti egység létszámától függően **2-3 évente az ellenőrzések során minden felhasználó jogosultsága ellenőrzésre kerüljön.**

g) **Minden ellenőrzés során felül kell vizsgálni** az adott szervezeti egységben dolgozó, adott szakrendszerekben, illetve az általánosan használt rendszerekben (pl. file-szerver, e-mail szolgáltatás, stb.) jogosított személyeket, a módosított jogosultsággal rendelkező, valamint és a szervezeti egységből korábban távozott felhasználók jogait.

h) Az ilyen jogosultság-megszüntetési cselekmények konkrét felsorolásával (ki, melyik rendszerben, milyen jogosultsággal rendelkezett, ebből mi került megszüntetésre) a fenti jegyzőkönyvet ki kell egészíteni.

i) Az ellenőrzés során felül kell vizsgálni a **30 napnál régebb óta nem használt** fiókokat. Ezeket az érintett szervezeti egység vezetővel történt egyeztetést követően le kell tiltani. Amennyiben az adott elektronikus információs rendszerben erre lehetőség van, automatizmusokat kell érvényesíteni a **30 napnál régebben nem használt fiókok letiltására**, kivéve ha írásos engedély van a további használatra.

j) A nyilvántartás ellenőrzésének rendje jelen Szabályzat kihirdetésével kerül kihirdetésre.

k) A nyilvántartás ellenőrzésének felülvizsgálata jelen Szabályzat felülvizsgálatával kerül felülvizsgálatra.

73. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

a) Hivatalban és a Hivatal eszközein, a Hivatal Információs Rendszerein vagy rendszerelemein azonosítás vagy **hitelesítés nélkül semmilyen tevékenység nem folytatható.**

b) Ez alól kivételt képeznek a belső hálózattól független, külső internetre csatlakoztatott:
- ügyfélterminálok
- a bizottsági és képviselő testületi felhasználók eszközei
- publikus honlap publikus funkciói

74. Rendszer- és kommunikációvédelmi eljárásrend, rendszer- és kommunikációvédelem.

a) Az elektronikus információs rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától.

b) Az elektronikus információs rendszer védi az érintett szervezet által meghatározott **maradvány információk** (pl.: átmeneti fájlok) bizalmasságát, sértetlenségét.

c) A Hivatal elektronikus információs rendszere meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást.

d) A Hivatal a rendszer és kommunikáció védelmét az alábbi eszközökkel biztosítja:
- biztonság tervezésére, értékelésére, elemzésére kialakított eljárásrenddel,
- a kritikus rendszerekre rendszerbiztonsági tervek kialakításával, bevezetésével, működtetésével,
- az alkalmazások, folyamatok szükséges mértékű szétválasztásával,

- a felelősségek, biztonsági funkciók, szétválasztásával,
- konfigurációkezelési és változáskezelési eljárásrenddel ,
- határvédelemmel, benne túlterhelés és szolgáltatás megtagadás alapú támadás elleni védelemmel,
- hozzáférési, hitelesítési eljárásrenddel ,
- hozzáférési pontok szigorú szabályozásával,
- karbantartási eljárásrenddel

e) Külső szolgáltatóval a szerződésben foglaltak szerint, titoktartási nyilatkozat megtételét követően ismertethető meg az eljárásrend.

f) **Eljárásrend felülvizsgálata, frissítése.** A rendszer- és kommunikációvédelmi eljárásrendet jelen Szabályzat felülvizsgálatával egyidejűleg felül kell vizsgálni. Amennyiben az indokolt, az eljárásrendet a Szabályzat módosításával kapcsolatos eljárásrend szerint frissíteni kell.

g) Jelen Rendszer- és kommunikációvédelmi eljárásrend jelen Szabályzat kihirdetésével kerül kihirdetésre.

75. Vezeték nélküli, mobil eszközök hozzáférése

a) Alapértelmezett tiltás.
A Hivatalban a belső informatikai hálózatra, elektronikus információs rendszerre és az NTG kapcsolatra tilos olyan **vezeték nélküli** hozzáférést biztosító eszközt telepíteni, amely jelentős mértékben megnöveli a bizalmasság, sértetlenség, rendelkezésre állás kockázatát.

Azaz nem okozhat adatvédelmi incidenst, amikor a Hivatal elektronikus információs rendszerében tárolt adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés következik be.

b) Külső hálózat használata.

- A vezeték nélküli hozzáférést igénylő és a hivatali elektronikus információs rendszeren keresztül végzett feladatokhoz, az érintett középvezető köteles legalább a külső hálózati jogosultságok gyakorlását **megelőző 3 munkanappal** a jogosultságot megigényelni.

- Az igénylésben meg kell határozni a hálózatra csatlakozók nevét, eszközét, eszközén található operációs rendszert, valamint a csatlakozás okát, időtartamát.

- A kapcsolat kizárólag VPN-en keresztül történhet.

- A kapcsolat az Üzemeltetési és Informatikai Csoportvezető írásbeli jóváhagyásával, és csak külső internetes hálózat útján biztosítható.

- Nem kell előzetesen engedélyeztetni a képviselők és a bizottsági tagok hozzáférését, ha a Hivatal által biztosított eszközzel kívánnak csatlakozni.

- Az informatikai hálózatban a külső internet kapcsolatot a belső hálózattól fizikailag és logikailag szeparált módon kell biztosítani.

- A két hálózatot tilos összekapcsolni!

76. A vezeték nélküli hozzáférést nyújtó eszközök konfigurálása

a) A vezeték nélküli hozzáférést nyújtó eszközöket – kivéve a publikus internet szolgáltatást nyújtó eszközök – úgy kell konfigurálni, hogy az csak titkosított módon, hitelesített felhasználókat vagy eszközöket engedjen hozzáférni a hálózathoz.

b) A hitelesítéséhez szükséges kódokat havonta meg kell változtatni a hálózatba kapcsolt minden vezeték nélküli eszközön. A kódok megváltoztatására csak a kijelölt informatikai ügyintéző jogosult védett hálózaton kialakított vezetékes kapcsolaton keresztül.

c) A wireless LAN és a WIFI, a Hivatal esetében együttesen kerül alkalmazásra a hálózati adatbiztonság érdekében.

77. Antennák, AP eszközök

A Hivatalban lehetőség szerint olyan karakterisztikájú és teljesítményszintű antennákat, AP eszközöket, és árnyékolási megoldásokat kell felszerelni, vagy egyéb technikai megoldásokat alkalmazni, amelyekkel csökkenthető az érintett szervezet fizikai védelmi határain kívül a jelek észlelésének valószínűsége.

78. Mobil eszközök hozzáférés ellenőrzése

a) A Hivatali munkavégzéshez csak hivatali tulajdonú, használatra átadott és a Hivatali informatikai ügyintéző által az Infrastruktúra tervben meghatározott mobil eszközökre vonatkozó alapkonfigurációval telepített eszközöket szabad használni.

b) A Hivatal tulajdonában lévő vagy a Hivatal adatait használó mobil eszközökön **gondoskodni kell az eszköztitkosításról, a tároló alapú titkosításról,** vagy más technológiai eljárást kell alkalmazni a mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

c) Az alapkonfigurációt tilos megváltoztatni, kivéve az alapkonfiguráció változására vonatkozó eljárásrend keretében történő változtatásokat.

d) **A Hivatali hálózathoz tilos saját eszközzel csatlakozni,** kivéve a különösen indokolt eseteket, amikor a külső munkatársakra vonatkozó engedélyeztetési folyamat, során a MAC cím alapján engedélyezett eszközöket meghatározott időtartamban, a meghatározott feladatok ellátására szabad csatlakoztatni.

e) A hozzáféréseket a határozott időtartam lejártával azonnali hatállyal meg kell szüntetni. Belső munkatárs saját eszközét (BYOD) különösen indokolt esetben a külső munkatárssal azonos biztonságú engedélyeztetési folyamat alapján, határozott időtartamra szabad csatlakoztatni.

79. Külső elektronikus információs rendszerek használata

Külső elektronikus információs rendszereket kizárólag a feladatellátás érdekében, a jogszabályi

felhatalmazás mértékéig szabad használni. Jogosultságot kérni, módosítani, törölni az e Szabályzatban meghatározott módon lehet, az 53-as pont alapján.

80. Felhasználói Internet böngészés, használat ellenőrzése

- A megtekintett oldalak, letöltések, illetve azok naplófájlja az Informatika számára hozzáférhető.
- Az Informatika köteles a naplók alapján az Internet forgalom követésére, mérésére, és a vezetőség kérésére arról részletes, az egyes munkaállomásokra, felhasználókra vonatkozó kimutatást készíteni.
- Az Üzemeltetési és Informatikai Csoportvezető, vagy az általa kijelölt személy köteles az Internet naplófájl alapján az Internet használatot ellenőrizni annak megállapítására, hogy az Internet használata megfelel-e a Hivatalbeli és a törvényi előírásoknak.
- Amennyiben az ellenőrzés nem megfelelő Internet használatot jelez, a vizsgálatot az érintett munkatárssal és vezetőjével ismertetni kell.
- Rendellenes esemény, adatvédelmi incidens, bekövetkezte vagy annak lehetősége, továbbá információbiztonsági veszélyeztetés esetén, az Információbiztonságért felelős személy haladéktalanul jelenteni köteles ezt a Jegyző, számára, továbbá szükség esetén a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet részére.

81. A felhasználók elektronikus levelezése.

a) A felhasználókra vonatkozó magatartási szabályokat a Szabályzat XVIII. fejezete tartalmazza, annak tartalmát az Üzemeltetési és Informatikai Csoportvezető által kijelölt informatikai ügyintéző belső oktatás keretében a felhasználókkal rendszeresen ismerteti.

b) A Hivatal jogosult az elektronikus levelező rendszerében továbbított üzenet vagy levél tartalmát, az üzenet vagy levél feladójának vagy címzettjének kiszolgáltatása nélkül, a Hatóság számára – kérésre – átadni.

c) Rendellenes esemény, adatvédelmi incidens, bekövetkezte vagy annak lehetősége, továbbá információbiztonsági veszélyeztetés esetén, az Információbiztonságért felelős személy jogosult az elektronikus levelek ellenőrzésére. Előzetes észlelés esetén haladéktalanul jelenteni köteles ezt a Jegyző számára, továbbá szükség esetén a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet részére.

82. Az elektronikus információs rendszer felügyelete.

a) A Hivatal határvédelmi eszközeit úgy kell beállítani, hogy az automatikusan, valós időben is alkalmas legyen a kibertámadások vagy a jogosulatlan hozzáférési kísérletek vagy hozzáférések észlelésére, azonosítására, valamint a megfelelő technikákkal felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre, vagy körülményre tekintettel.

b) A Hivatalban alkalmazott elektronikus információs rendszereket és határvédelmi eszközöket úgy kell beállítani, hogy azok alkalmasak legyenek a jelen Szabályzatnak megfelelő naplóbejegyzések készítésére amely **naplóbejegyzéseket a megfelelő eljárásrenddel véd a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.**

c) A felügyeleti eszközt úgy kell beállítani, hogy szokatlan vagy magas kockázatú tevékenység esetén **TELEGRAM és e-mail felületeken egyaránt riassza az Informatika kijelölt ügyintézőjét,** aki köteles megvizsgálni a naplóbejegyzéseket és köteles fokozott védelmi intézkedéseket tenni a kibertámadások megelőzése érdekében.

d) A naplóbejegyzéseket a napló kiértékelés fejezetben foglaltak szerint folyamatosan ellenőrizni kell.

83. Biztonsági riasztások és tájékoztatások

a) A Hivatal a biztonsági riasztások kommunikálására a Telegram alkalmazást használja, melyben minden riasztás visszakereshető.

b) Az Információbiztonságért felelős személy folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, valamint a Hatóságtól érkező értesítéseket; ezek tartalmáról tájékoztatja az Informatika munkatársait.

c) Amennyiben a figyelmeztetések és/vagy értesítések a felhasználókra vonatkozó információkat tartalmaznak, úgy a figyelmeztetést az Informatikai Csoport haladéktalanul közzéteszi az Intranet belső webszerveren.

84. Adathordozó szállítás, Állami Futárszolgálat általi szállítás, ellenőrzés, címkézés eljárásrendje

a) A hivatalban alkalmazott karbantartás, szállítás, stb. során használt, hivatali rendszerek és rendszerelemek, különösen a hivatali adatokat tartalmazó adathordozók kizárólag az Üzemeltetési és Informatikai Csoport vezetőjének vagy akadályoztatása esetén a helyettesének engedélyével szállíthatók el.

b) Az adathordozók elszállítását megelőzően – feltéve, hogy az adathordozó elszállításának nem az adatok jogszerű és tervezett átvitele a cél – az Informatika ellenőrzi az elszállítandó adathordozókat az alábbiak szerint:

- visszaállíthatatlanul törölni kell az adatokat a rendszerelemekről és az adathordozóról (az adathordozó törlése nem eredményezheti a szükséges adatok elvesztését, azokat a megfelelő helyre le kell menteni a beavatkozást megelőzően),
- meg kell győződni arról, hogy az adathordozó nem tartalmaz visszaállítható adatokat,
- az adathordozó selejtezésekor az adathordozót fizikailag meg kell semmisíteni,
- a megsemmisítésre vagy elszállításra váró adathordozókat, az esemény bekövetkeztéig elzártan, csak az Üzemeltetési és Informatikai Csoportvezető és Helyettese által hozzáférhetően kell tárolni,
- tűzálló páncél burkolatban kell szállítani.

c) Az érintett szervezet alapértelmezésben tiltja, indokolt esetben az Üzemeltetési és Informatikai Csoportvezető engedélyével, nyilvántartás vezetése és informatikai ügyintéző felügyelete mellett szállíthatók informatikai eszközök a Hivatalba, illetve a Hivatalból el.

d) A létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást a portaszolgálat figyeli és ellenőrzi.

e) A 466/2017. (XII. 28.) Korm. rendeletben meghatározott adattrezor-archiválást tartalmazó fizikai adathordozókat, az ún. KAT konténereket, a Készenléti Rendőrség Különleges Szolgálatok Igazgatósága Állami Futárszolgálat regisztrált képviselői vehetik át; illetve az Informatika részéről ezzel írásban megbízott személyek adhatják át.

f) Az Üzemeltetési és Informatikai Csoport vezetője jogosult rendszeres és időközi adattrezor-archiválást elrendelni, továbbá ő vagy az általa kijelölt személy köteles bejelenteni a Készenléti Rendőrség Különleges Szolgálatok Igazgatósága Állami Futárszolgálatánál a konténer szállítási igényt. Az adatküldés havonta egyszer történik.

g) A KAT konténerekben levő adathordozók átadás-átvételének helyszíne az Informatika-helyisége, ahol kizárólag a Futárszolgálat regisztrált képviselői az azonosításuk után és a Hivatal részéről ezzel megbízott személyek tartózkodhatnak

h) Az adathordozók átadás-átvétele erre a célra kialakított és a Futárszolgálat által rendszeresített 1 db plombával ellátott, lezárt KAT konténerben történő elhelyezéssel, valamint a futárjegyzék kitöltésével és annak kölcsönös aláírásával történik.

i) A KAT konténerben külön lezárt, a ragasztásnál a megbízott munkavállaló által szignózott borítékban kell elhelyezni:
- a fizikai adathordozók gyári számát,
- a titkosított és mentett adatok feloldását biztosító jelszót és
- az archivált rendszerek gyári nyilvántartó jegyzékét.

j) Az adathordozóknak a Hivatalba való rendszeres visszaszállítása az előzőek szerint, erre a célra kialakított és a Futárszolgálat által rendszeresített KAT konténerben történő elhelyezéssel, továbbá annak leplombálásával, valamint a futárjegyzék kitöltésével és kölcsönös aláírásával történik.

k) Ha nyilvánvaló rendellenesség észlelhető az adattrezor-archiválást tartalmazó fizikai adathordozók átadás-átvételével, dokumentálásával, a KAT konténerrel, a fizikai adathordozóval és a plomba fizikai állapotával kapcsolatban, akkor az Informatika megbízott munkavállalói jegyzőkönyvet kötelesek felvenni.

l) A kitöltött futárjegyzéket, a fizikai adathordozók gyári számát és az archivált rendszerek gyári nyilvántartását az Informatika munkatársai hiteles papír alapon kötelesek megőrizni.

85. Az elektronikus információs rendszer mentései, Kormányzati adattrezor-archiválás

a) A Hivatalban lévő adatok mentése az Informatikafeladata. A mentések napi, heti havi rendszerességgel kerülnek elvégzésre.

b) A mentett adatok, információk és bizalmas informatikai elemek mentésekor mind a fizikai hozzáférési, mind az elektronikus vagy fizikai tárolási mind pedig az adathordozókra vonatkoztatva – jelen Szabályzatban meghatározott módokon – meg kell őrizni a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos helyszínen.

c) A Hivatal az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendeletben meghatározott adattrezor-archiválást is végez.

d) A Jegyző az elektronikus információs rendszer kockázatelemzésének eredményeként az adattrezor-archiválásban érintett adatokat a 3. számú osztályba sorolta.

e) Az Üzemeltetési és Informatikai Csoport vezetője jogosult rendszeres és időközi adattrezor-archiválást elrendelni. Az adattrezor-archiválásban érintett adatokat a 3. számú kategóriának megfelelően a szerverüzemeltetők fizikai adathordozóra menteni kötelesek, ezt megelőzően az adatokat partíció titkosítással védik le.

f) A fizikai adathordozók gyári számát, a titkosítást feloldó jelszót és az archivált rendszerek azonosítóit nyilván kell tartani; mindezek jegyzékét az Informatika őrzi.

86. Adathordozók kezelése, titkosítása, törlése, megsemmisítése, selejtezése

a) Az adathordozókat alapértelmezésben a Hivatal addig használja, amíg az hardveresen támogatott vagy amíg a tárolókapacitása elégséges, illetve amíg az eszköz hibátlanul működőképes.

b) A Hivatal vonalkóddal megjelöli az elektronikus információs rendszer adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket, ha ezek rendelkezésre állnak.

c) A Hivatal meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz.

d) Azokat az adathordozókat, amelyeket a Hivatal a munkavégzéshez, illetve a feladatellátásra alkalmatlannak minősített, a selejtezési eljárást:
   - az adattartalmat törölni kell,
   - fizikailag meg kell semmisíteni és / vagy
   - veszélyes hulladékok kezelésére jogosult vállalkozást megbízni az elszállításával, amelyről a vállalkozásnak szállító jegyet kell kiállítani.

e) A használhatatlan adathordozók adatmegsemmisítés (törlés) nélkül nem kerülhetnek ki a Hivatal területéről.

f) Az adatmegsemmisítést úgy kell elvégezni, hogy a tárolt adatoktól függetlenül azok visszaállíthatatlanok

legyenek.

g) A törölt adathordozókról minden esetben a legkorszerűbb, rendelkezésre álló technológiával ellenőrizni kell az adatok visszaállíthatatlanságát.

h) Amennyiben az adatok egészét vagy részét sikerül visszaállítani, úgy az eljárást felül kell vizsgálni, az alkalmazott technológiát ki kell cserélni olyan megoldásra, amellyel biztosítható az adatok visszaállíthatatlan törlése.

i) Az adathordozót addig tilos kiadni, amíg az visszaállítható adatokat tartalmaz.

j) Adathordozók fizikai megsemmisítése.
   - Az adathordozókat – amennyiben a felépítésük azt engedi – alkotóelemeire szét kell szerelni, és az adathordozó réteget roncsolásos technológiával le kell fejteni az eszközről.

   - Amennyiben ez nem lehetséges, úgy az adathordozót fizikailag több részre mechanikai behatás útján szét kell törni.

k) A megsemmisítést, a megsemmisítésre való átadást, az adathordozók, eszközök azonosíthatóságát dokumentálni kell.

87. Az elektronikus információs rendszer elemeinek hulladékgyűjtése és elszállítása

a) Az elektronikus információs rendszer hulladéknak minősülő elemeit, tartozékait – különös tekintettel az akkumulátorokra – szállító és csomagoló anyagait a Hivatalnak telephelyenként meghatározott és biztonságos helyen kell tárolnia.

b) Az Üzemeltetési és Informatikai Csoportvezető köteles a Jegyző felé javaslatot tenni a hulladékoknak és veszélyes hulladékoknak, a 2012. évi CLXXXV. törvényben, a 225/2015. (VIII. 7.) Korm. rendeletben foglalt előírásoknak megfelelő, elszállítására vonatkozóan.

c) Az elszállítás folyamatát az Informatika-dolgozóinak dokumentálniuk kell.

88. Megbízhatósági és sértetlenségi teszt

a) Az Informatika teszteli a biztonsági mentéseket az adathordozók megbízhatóságának és az információ sértetlenségének a garantálása érdekében.

b) Tesztnek minősül az a nem tervezett eljárás is, amely során a hivatali munkavégzéshez szükséges adatok visszaállítása felhasználói kérésre történik.

c) A Hivatal az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet szerint visszaszállított fizikai adathordozókról az adat-helyreállítást kizárólag a Jegyző utasítására lehet elvégezni.

d) Az Adattrezor adathordozóinak adat-helyreállítását kizárólag a kijelölt munkaállomásokon lehet elvégezni.

89. Kártékony kódok elleni védelem, vírusvédelem

a) Hivatal a kártékony kódok elleni védelmi intézkedésként kereskedelmi forgalomban kapható és/vagy nyilvánosan hozzáférhető nyílt forráskódú kémprogram- és vírusirtó rendszereket, valamint biztonsági frissítéseket és javítócsomagokat alkalmaz a kliens és a szerver gépeken. A kártékony kódok elleni védelem csak az Alkalmazáskatalógus dokumentumban meghatározott védelmi szoftverekkel végezhető.

b) Ezek telepítése és konfigurálása csak az Üzemeltetési és Informatikai Csoportvezető által kijelölt informatikai ügyintéző által történhet. Az informatikai ügyintéző ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

90. Kliens számítógépek kártékony kódok elleni védelmi feltételei

a) Kliens számítógépeken olyan kártékony kódok elleni védelmet kell alkalmazni, amelyhez legalább napi szintű adatbázis-frissítés érhető el.

b) Az Informatika–által beszerzett védelmi rendszer legyen megbízható, az adatbázis-mintákon kívül legyen lehetőség különböző szintű heurisztikus keresés beállíthatóságára.

c) A rendszer védje a saját állományait a kompromittálódás ellen, csak a rendszergazda által személyesen eszközölt cselekményeket engedélyezze. Felhasználó vagy alkalmazás ne legyen képes a rendszert átkonfigurálni (parancssorból vagy szkriptek futtatásával sem), a szolgáltatásokat leállítani.

d) Az ellenőrzés folyamatosan történjen a háttérben, folyamatosan legyen megfigyelt a számítógép memóriája. Háttértároló csatolásakor automatikusan induljon el az ellenőrzés, a levelezőprogram használatakor, a csatolt mellékletek letöltésekor, webböngészéskor és más, interneten végzett cselekmények hatására várható fertőzésveszélyes eseményekkor, programok, futtatható állományok szkriptek elindításakor, fertőzhető adatállományok használatakor történjen meg a teljes körű ellenőrzés.

e) A fertőzött állományokat az informatikai üzemeltető tisztítsa meg, ha erre nem képes, helyezze karanténba, egyidejűleg küldjön riasztást az informatikai ügyintézőnek.

f) Az adatbázist legalább naponta frissítse, legyen képes belső hálózaton található proxy szerverről begyűjteni és telepíteni a frissítéseket és a konfigurációkat. Csak ellenőrzött frissítéseket fogadjon be.

g) A kliens számítógépeken futó alkalmazások biztonsági frissítéseit az üzemeltetőknek folyamatosan telepíteni kell.

h) Külön biztosítani kell az Informatikának olyan hordozható és asztali számítógép kártékonykód-mentességét, amelyek nem csak a hivatali hálózatban és / vagy a hálózattól leválasztva üzemelnek. Ezeknél a számítógépeknél meg kell oldani az adatbázis-frissítést a hivatali hálózattól eltérő hálózatok használata esetére is.

91. Szerver számítógépek kártékony kódok elleni védelme.

a) A szervereken és a központi információs rendszereken a Informatika a meghatározott szolgáltatásokkal rendelkező, olyan kártékony kódok elleni védelmi szoftvertermékét kell alkalmazni, amely központilag képes folyamatosan monitorozni a hálózatban és a szerver-szolgáltatások által kezelt állományok és csomagok kártékonykód-mentességét, különösen a belépési és kilépési pontokon.

b) Amennyiben kártékony kódot vagy arra utaló jeleket tapasztalnak az üzemeltetők, akkor felderítik és megsemmisítik (hatástalanítja) azokat.

92. Kéretlen üzenetek elleni védelem

a) A Hivatal elektronikus információs rendszere az elektronikus levelezés során mind a bejövő mind a kimenő kéretlen üzenetekkel, illetve a levélszeméttel kapcsolatos központi védelmi megoldásokat valósít meg a rendszer ki- és belépési pontjain az alábbiak szerint:

- szűri a leveleket a tárgyban szereplő kifejezések alapján
- szűri a leveleket a levél tartalmában szereplő kifejezések alapján
- feketelisták alapján szűri a leveleket
- gyakori levélszemét-minták alapján szűri a leveleket.

b) A kiszűrt leveleket a rendszer még a felhasználóhoz történő megérkezését megelőzően karanténba helyezi, majd 60 nap elteltével törli. A törölt levelekről nem küld értesítést sem a feladónak sem a címzettnek.

93. Frissítés a Kéretlen üzenetek elleni védelme miatt

a) Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival és elérhető adatbázisaival.

b) Szükség esetén az Informatika frissíti a levélszemét-ellenőrző és -szűrő rendszerét a **konfigurációkezelési eljárásrend szerint.** A változásokat át kell vezetni az Alkalmazáskatalóguson.

94. Naplózási és elszámoltathatósági eljárásrend kihirdetése

a) A Jegyző az elektronikus információs rendszereiben történt események és incidensek vizsgálata érdekében az alábbi **naplózási és elszámoltathatósági eljárásrendet határozza meg.**

b) A naplózási elszámoltathatósági eljárásrendet az Üzemeltetési és Informatikai Csoport vezetője jelen Szabályzat megismertetésével az informatikai ügyintézők, valamint a rendszer működéséért felelős külső szervezetek számára kihirdeti.

c) A jelen Szabályzatban foglalt eljárásrend megismerését az **üzemeltetésben részt vevők** – külső szolgáltatás igénybe vétele esetén a kijelölt kapcsolattartók útján – **aláírásukkal igazolják.** Az aláírt nyilatkozatokat az Üzemeltetési és Informatikai Csoportvezető zárt páncélszekrényben őrzi.

95. Naplózási eljárásrend

a) **A naplózási eljárásrendet,** valamint a naplózandó eseményeket a Hivatal jelen Szabályzat felülvizsgálatakor vagy a naplózási rendben történő változások esetén **felülvizsgálja és frissíti.**

b) A naplózandó események vizsgálatakor egyeztetni kell a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, **a kölcsönös támogatás növelése** érdekében, valamint, hogy iránymutatással segítse a naplózható események kiválasztását.

c) Meg kell vizsgálni továbbá, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő **tényfeltáró vizsgálatok támogatásához.**

d) A Hivatalban alkalmazott elektronikus információs rendszerekre vonatkozóan elő kell írni, valamint **a rendszereket alkalmassá kell tenni az alábbi naplógenerálási feladatok végrehajtására.**

96. Naplózandó események, naplógenerálási feladatok

a) A Hivatali Informatika köteles olyan naplóbejegyzéseket előállítani a következő eseményekre:
- adatokhoz való hozzáférés (ki, mikor, mit látott, módosított)
- felhasználói bejelentkezés, kijelentkezés,
- felhasználók által végzett tranzakciók
- felhasználó jogosultsági szintjének változtatása,
- rontott jelszó megadás,
- jelszó-változtatás, resetelés
- jogosultságcsoportok módosítása
- felhasználó létrehozása, törlése
- felhasználók által végzett tranzakciók
- felhasználói kvóták megsértése

b) Az informatikai rendszernek alkalmasnak kell lenni arra, hogy felügyelhető legyen, hogy az események melyik csoportját a rendszer melyik különálló összetevője naplózza.

97. A naplóbejegyzések tartalma

a) Az elektronikus információs rendszereket úgy kell paraméterezni, hogy a naplóbejegyzésekben elegendő információt gyűjtsenek be ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

b) Az informatikai rendszer lehetőséget nyújt arra, hogy a **fentieken túl, részletesebb információkat** is be lehessen venni, a naplóbejegyzések típusa, elhelyezkedése vagy tárgya alapján, amennyiben erre szükség mutatkozik. További naplózási események beállításakor figyelemmel kell lenni a továbbiakban előállítandó naplók mennyiségére a **tárkapacitás** és a feldolgozás vonatkozásában, és csak a védelemmel arányos módon szabad engedélyezni.

c) A naplóbejegyzésnek a következő adatokat mindenképp tartalmaznia kell:
- felhasználói név, azonosító,
- az esemény dátuma és időpontja (eltérés esetén a rögzítés időpontja is),
- munkaállomás azonosítója,
- az esemény leírása,
- az esemény sikeressége, vagy sikertelensége,

- file hozzáférés esetén, a file neve.

d) A rögzített adatok alapján meg kell tudni határozni, hogy:
   - egy bizonyos adathoz egy konkrét időpillanatban ki fért hozzá;
   - egy bizonyos személy adott időintervallumban milyen adatokhoz fért hozzá.

98. Napló tárkapacitás

a) Új rendszerek beállításakor, valamint a jelenleg hasznát rendszerek felülvizsgálata során meg kell határozni, hogy a minden alkalmazott elektronikus információs rendszerhez implementálva lett-e a **megfelelő méretű napló tárhely.**

b) A napló tárkapacitást minden esetben úgy kell kialakítani, hogy az a jelen Szabályzatban meghatározott naplózási kritériumrendszernek megfeleljen.

c) A napló tárkapacitást **úgy kell méretezni, hogy minden naplóbejegyzés a keltezésétől számított 1 évig visszakövethető legyen.**

99. A naplózási incidens, a riasztás, a felügyelet

a) Amennyiben a naplózás **valamilyen hiba** okán nem tud megtörténni, a felügyeleti rendszer azonnal **Telegram és e-mail riasztást küld** a rendszer üzemeltetéséért felelős informatikai ügyintéző számára, aki azonnali hatállyal megvizsgálja a napló hibának okát és javítja a hibát.

b) A felügyeleti rendszer ezzel egy időben megkezdi a naplózási folyamat szabályos leállítását. Az informatikai ügyintéző köteles a hiba elhárítását követően a naplózást visszakapcsolni és a teljes körű naplózás működését mintavételezéssel ellenőrizni.

c) Amennyiben a napló tárhely beteléshez közelít, azaz a **tárhely foglaltsága eléri a rendelkezésre álló kapacitás 80%-át, a felügyeleti rendszer valós idejű riasztást küld** a rendszer üzemeltetéséért felelős informatikai ügyintéző számára, aki azonnali hatállyal megvizsgálja a tárhely kapacitásának növelési lehetőségeit, és végrehajtja a legkevesebb veszteséggel járó műveletet (pl. tárhely kapacitás növelés, archiválás, tömörítés, 1 évnél régebbi adatok törlése)

100. Naplóvizsgálat és jelentéskészítés

a) Hivatal az elektronikus információs rendszerei által készített naplók folyamatos ellenőrzésére és kiértékelésére speciális, integrált, minden rendszerből származó összesített naplókiértékelésre alkalmas naplókiértékelő rendszer szoftvertermékét és szolgáltatást vesz igénybe.

b) A naplókiértékelő rendszerrel szemben támasztott követelmények:
   - Nagy sebességű log-feldolgozást biztosít,
   - Beépített vagy szabadon készíthető logdefiníciók segítségével felismeri, felbontja, indexeli és tárolja a naplósorokat,
   - Biztosítja egyedi alkalmazások naplóinak feldolgozását,
   - Webes kezelőfelülete nyújt az adatok hatékony eléréséhez,
   - Multi-dimenzionális statisztikai adatokat gyűjt valós időben, bármely logsor bármely mezőjét

felhasználva,

- Biztonságos csatornán továbbítja a logokat más eszközöknek,
- Exportálható jelentéseket gyárt automatikusan PDF formában,
- Riasztásokat küld egyedileg meghatározott feltételekre illeszkedő logok esetén,
- Egymástól független logsorok közötti összefüggéseket talál, korrelációs elemzést végez valós időben,
- Syslog, rsyslog, syslog-ng, Lasso, Snare kompatibilis,
- SOAP API interfészt ad a külső programoknak,
- tömörítetten tárolja a naplóbejegyzéseket

c) A naplókiértékelő rendszer által generált naplókat minden informatikai ügyintéző az általa – valamint a munkaköri leírása szerint – üzemeltetett rendszerek vonatkozásában napi szinten köteles átnézni, **nem megfelelő vagy szokatlan működésre utaló bejegyzések észrevételezése esetén, illetve riasztáskor a naplóbejegyzések tartalmát kiértékelni és megkezdeni a probléma okának feltárását, a rendellenes működés megszüntetését.**

d) Egyidejűleg az informatikai ügyintézők kötelesek tájékoztatni az Információbiztonságért felelős személyt, aki megteszi a szükséges – rendellenes működés kockázatával arányos – lépéseket.

101. Naplóbejegyzések védelme, sértetlensége

a) Az elektronikus információs rendszer által generált naplókat, valamint a naplókiértékelő rendszer által készített riportokat úgy kell tárolni, hogy ahhoz illetéktelen személyek ne férhessenek hozzá, ne módosíthassák és ne törölhessék.

b) Az elektronikus információs rendszereket és a naplókiértékelő rendszereket úgy kell jogosítani, tárolni és paraméterezni, hogy ahhoz naplómódosítási vagy törlési céllal illetéktelenek ne férhessenek hozzá.

c) A naplóbejegyzéseket és a naplókiértékelő rendszer által készített riportokat, valamint a naplót készítő alkalmazások és rendszerek naplózással kapcsolatos beállításait a tartalék telephelyre is alkalmazni kell.

102. Rendszeridő beállítás, szinkronizálása

a) Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

b) Rendszeridő beállítása. A Hivatal az elektronikus információs rendszerei, valamint a kliens számítógépek rendszerórájának beállításához az UTC időt szolgáltató hálózati idő protokollt (Network Time Protocol, NTP) használ.

c) A rendszerórákat úgy kell beállítani, hogy egy folyamatosan háttérben futó alkalmazás kiszámítja a rendszeróra elcsúszását, és folyamatosan módosítja azt.

d) Ennek eredményeképp nem lesznek naplózási szempontból kezelhetetlen méretű javítások, amelyek inkonzisztens naplókat eredményezhetnének (ntpd).

e) Időbélyegek Az alkalmazott elektronikus információs rendszerek az előző pontban meghatározott időszinkron útján beállított belső rendszerórát használnak a naplóbejegyzések időbélyegeinek előállítására.

103. Határvédelem

A Hivatal saját maga, **folyamatos tűzfal üzemeltetési support szolgáltatást lát el**, ezen belül:

- a szolgáltatásokhoz szükséges szoftverek üzemszerű működésének folyamatos biztosítását;
- a tűzfalak konfigurációs állományainak napi szintű mentését a Vállalkozó központi management rendszerébe (e rendszer hatékony mentési és katasztrófa elhárítási képességeinek köszönhetően az üzemeltetett rendszer teljes megsemmisülése esetén is rövid időn belül visszaállítható a produktív környezet)
- a tűzfalak naplófájljainak rendszeres figyelését;
- a felfedezett, rendellenességekre utaló jelekről jelentés készítését, illetve amennyiben az a rendszeren belüli módosítással megoldható, akkor annak kivitelezését;
- napi fájlrendszer integritás ellenőrzés;
- a naplóállományok forgatását, biztonságos archiválását;

- statisztikák készítését azokon keresztül az adott szolgáltatás ellenőrzését;
- a biztonsági szoftverfrissítések elvégzését;
- az időszakosan teljes frissítést (összes szoftver és kernel);
- online elérés esetén az Internet felől elérhető szolgáltatások, a fájlrendszer-telítettség, a hálózati interfészek hibái, a futó folyamatok, az entrópia pool, a terhelés (load), a levelező spool-ok telítettsége, a memóriatelítettség, a nyitott fájlok, a belépett felhasználók, a legtöbb memóriát fogyasztók tízes listája, a törölt futtatható állományok folyamatos ellenőrzését

Amennyiben a szoftver a rendszerben változást észlel, vagy olyan eszközöket talál, amelyek régóta nem kerültek bekapcsolásra vagy csatlakoztatásra, úgy elektronikus levélben riasztást küld az üzemeltetőnek, aki az eltérő rendszerelemeket azonnali hatállyal megvizsgálja.

104. Internetcsatlakozás korlátozásai

a) A Hivatal a Nemzeti Távközlési Gerinc (NTG) szolgáltatáshoz 1 db fizikailag kiépített, az Informatikai Csoport szerverszobájában elhelyezett, a NISZ Zrt. által felügyelt határvédelmi eszközökön keresztül létesített csatlakozáson kapcsolódik az internet és más külső kommunikációs szolgáltatáshoz.

b) A Hivatal viszonylatában az NTG üzemeltetője: a Nemzeti Infokommunikációs Zrt. (NISZ), aki a csatlakozáshoz szükséges IP címeket, és a két hálózat közti kapcsolatot biztosítja saját tűzfalrendszerén keresztül. A Hivatal működéséhez szükséges router saját tulajdonú, mivel üzemeltetést csak Cisco eszközre vállalja a NISZ Zrt., ezért az NTG határt a router jelenti.

c) **Tilos olyan hálózati csatlakozás kialakítása,** (az ahhoz csatlakoztatott bármely eszközzel összekapcsolva pl. modemes, mobiltelefonos, mobilinternetes, bluetooth, WiFi vagy vezetékes, illetve bármilyen arra alkalmas technológia alkalmazásával) a belső hálózathoz, ami jelentős mértékben megnöveli a bizalmasság, sértetlenség, rendelkezésre állás kockázatát.

d) Nem okozhat adatvédelmi incidenst, amikor a Hivatal elektronikus információs rendszerében tárolt adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés következik be.

105. Más hálózati kapcsolatok korlátozásai

a) Más hálózatok közvetlen csak a határvédelmi megoldásokon kívülre csatlakoztathatók a jelen Szabályzatban meghatározott, megfelelő felügyeleti, ellenőrzési és védelmi, valamint az infrastruktúra tervben meghatározott forgalomáramlási szabályok beállítását követően.

b) **A forgalomáramlási szabályok** közül az ideiglenesen vagy tartósan beállított kivételt annak időtartama feltüntetésével dokumentálni kell.

c) A kivételek lejártakor, valamint havi rendszerességgel át kell tekinteni a forgalomáramlási szabályokat, és el kell távolítani minden olyan kivételt, amely időtartama lejárt, vagy amely jelenlétét az alapfeladat ellátása nem indokolja.

106. Távoli készülékek

a) Alapesetben távoli készülékkel elektronikus rendszerhez kapcsolódni tilos!

b) Az elektronikus információs rendszerhez kizárólag az engedélyezett VPN-en keresztül lehet távoli készülékkel kapcsolódni.

c) Amennyiben az ilyen kapcsolat elengedhetetlen, úgy **meg kell gátolni, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel.**

107. Túlterhelés – szolgáltatás megtagadás alapú támadás – elleni védelem

Hivatal internetes kapcsolatán, valamint a kívülről csatlakoztatott hálózati kapcsolatain olyan határvédelmi eszközöket kell üzemeltetni, amelyek **képesek megfelelő védelmet nyújtani a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben**, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján legalább az alább meghatározott biztonsági intézkedések bevezetésével:

- **alkalmazások blokkolása**: IDS behatolásvédelmi rendszerrel szűrje ki a túlterheléses támadások eszközeit alkalmazásszinten (kívülről befelé és bentről kifelé irányuló támadások esetén is)
- **kapcsolatszám korlátozása**: tiltsa ki az egy távoli végpont felől érkező indokolatlanul nagy számú kéréseket
- **lekérdezések számának korlátozása**: korlátozza az egy végpont felől védett alkalmazás-protokollokon (például HTTP, DNS) érkező lekérdezések számát
- **nem szabályos forgalom kiszűrése**: szűrje ki a hamis vagy gyanús kapcsolatokat, végezzen ellenőrzést a hibás, átlapolódó visszajátszott vagy nem szabványos hálózati csomagokra nézve és szűrje ki azokat (spoofing)
- **ismert szerverek tiltása:** adatbázisok alapján tiltsa a potenciális támadásokat okozó szervereket.

108. A határok védelme

a) Hivatal internetes kapcsolatán, valamint a kívülről csatlakoztatott hálózati kapcsolatain olyan határvédelmi eszközöket kell üzemeltetni, amelyek képesek megfelelő védelmet nyújtani az elektronikus információs rendszerei bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzésére.

b) Ennek érdekében a határvédelmi megoldás felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt az alábbiak szerint:
   - IPS/IDS
   - IDM
   - DLP
   - transzparens proxy

   A határvédelmi eszközök kialakítását és beállításait az **Infrastruktúra Terv tartalmazza.**

109. Szolgáltatások szétválasztása

a) Határvédelmi és felügyeleti eszközök

A határvédelmi és felügyeleti rendszerek még részben sem futhatnak olyan hardver eszközön, amelyen fizikailag vagy virtualizációs technológiával más, a hivatal belső vagy külső szolgáltatásokat nyújtó rendszerei futnak, még akkor sem, ha a logikai szeparáció biztonságos technológiával történik.

b) Statikus tartalomszolgáltatás

- A Hivatal működtetésében lévő, statikus (főleg kézi feltöltésű) vagy kvázi statikus (nem közvetlen belső hálózati eszközről származó automatikus adatszolgáltatás esetén) tartalomszolgáltatásra szolgáló webszervereket fizikailag szeparált módon, különálló szervereken kell futtatni, tehát az elektronikus információs rendszer **elkülönített végrehajtási tartományt tart fenn** a végrehajtó folyamatok számára.

- Nem futtathatók a webszerverek olyan virtualizált környezetben, amely azonos hardverre került telepítésre belső hálózati szolgáltatást nyújtó szerverrel, még akkor sem, ha azok logikailag biztonságos technológiával kerültek elválasztásra.

- Az ilyen szervereket a hivatali NTG kapcsolattól teljesen független internet kapcsolaton és határvédelmi megoldásokon keresztül kell üzemeltetni.

c) Nyilvános adattartalmak hozzáférése

A belső hálózati rendszerekből adatot szolgáltató, nyilvánosan hozzáférhető rendszerelemeket ún. demilitarizált zónákban (DMZ) kell elhelyezni, úgy, hogy a publikusan hozzáférhető eszközök csak ellenőrzött módon, irányított lekérdezéseket végezhetnek a belső szerverek felé. Minden más, a belső hálózat irányába történő lekérdezési és egyéb hozzáférési lehetőséget tiltani kell!

d) Elektronikus levelezési szolgáltatás

- Az elektronikus **levelezési szolgáltatást** úgy kell beállítani, hogy azon keresztül csak a rendszerbe ténylegesen létező elektronikus levelezési fiókkal rendelkező, és azon keresztül hitelesített és azonosított felhasználó legyen képes elektronikus levelet küldeni. A levelező rendszert webmail klienssel lehet elérni a belső hálózatból.

- A külső hálózatban tilos domain névvel azonosítani a webmail-es levelező szolgáltatást, azt csak IP cím alapján lehet elérni. A webmail szolgáltatás kívülről csak többtényezős, eszköz alapú hitelesítési eljáráson keresztül, legalább https biztonságú protokollon keresztül érhető el, ahol az eszköztől a kulcs nem választható el.

110. Rendszer-, információ- és adatátvitel sértetlenségének védelme, Rendszer és információsértetlenségi eljárásrend

a) A Hivatal a következő **titkosítási előírásokat** szabja meg a kliensek, felhasználók számára, különösen, ha valószínű a szervezeti adatátadás:

- bizalmas adatok kezelése esetén a felhasználó alkalmazza a „keepass" technikai lehetőségeket, tehát a a jelszavai biztonságos tárolását;
- alkalmazza a veracrypt szoftvereket, amelyek könnyen használhatók, nyílt forráskódúak és mindhárom nagy platformra elérhetőek és a segítségével titkosított konténerfájlokat hozhatnak

létre és létező partíciókat titkosíthatnak le.
- A feloldó kulcsot a két szintű biztonságnak megfelelően személyesen vagy TELEGRAM-ben kell a kliens részéről eljuttatni az általa megjelölt és biztonságosnak minősített célszervezet képviselőjének. Ezzel bizonyos szempontból mobilitást is kap az alkalmazott biztonsági eljárás.

b) Belső hálózati felhasználói alkalmazás hozzáférés a felhasználói alkalmazás használatát biztosítja, ami a felhasználói terület erre jogosult munkatársának a megfelelő azonosítási és hitelesítési eljárást követően a munkaállomásán rendelkezésre áll.

c) Belső hálózati privilegizált szolgáltatás hozzáférés a speciális informatikai szolgáltatások (pl. Internet, Laptop használat) igénybe vételét biztosítja.

d) Belső hálózati privilegizált üzemeltetői hozzáférés a Rendszerszoftverekhez (operációs rendszerek) és a rétegszoftverekhez (adatbázis-kezelők) való hozzáférést biztosítja, valamint a felhasználók felhasználói alkalmazásbeli hozzáférési jogosultság beállítását teszi lehetővé. Ilyen jogosultságokkal a kinevezett üzemeltetők rendelkeznek.

e) A Hivatal a rendszer és információ sértetlenségét az alábbi (megelőző, észlelő és kezelő) eszközökkel biztosítja:
- fizikai és környezeti védelmi intézkedésekkel
- hozzáférések szabályozásával
- vírusvédelemmel
- a biztonsági frissítések mielőbbi és felügyelt elvégzésével
- a működő rendszerek monitorozásával és riasztási rendszerrel
- naplózással és napló elemzéssel
- határvédelemmel és
- biztonsági események kezelésére kialakított eljárásrenddel,
- külső szolgáltatás során alkalmazandó eljárásrenddel

f) Külső szolgáltatótól igénybe vett elektronikus információs rendszer szolgáltatás esetén az eljárásrend betartását a külső szolgáltatóra nézve **szerződéses kötelemként érvényesíteni kell.**

g) Jelen Rendszer és információsértetlenségi eljárásrendtől közös megegyezéssel el lehet térni abban az esetben, ha a külső szolgáltató / üzemeltető:
- a rendszerhez megfelelő eljárásrendet készített, és az a Hivatal számára elfogadható, a védelemmel arányos intézkedéseket tartalmaz vagy
- a szolgáltatás igénybe vételét jogszabály írja elő

h) A Hivatal iroda- és csoportvezetői kötelesek a külső szolgáltatókkal / üzemeltetőkkel kapcsolatos együttműködésüket az Informatika felé haladéktalanul jelezni.

i) Rendszer és információsértetlenségi eljárásrend kihirdetése
Jelen rendszer- és információ sértetlenségre vonatkozó eljárásrend jelen Szabályzat kihirdetésével kerül kihirdetésre. Külső szolgáltatóval a szerződésben foglaltak szerint, titoktartási nyilatkozat megtételét követően ismertethető meg az eljárásrend.

j) Rendszer és információsértetlenségi eljárásrend felülvizsgálata, frissítése
A rendszer- és információsértetlenségi eljárásrendet jelen Szabályzat felülvizsgálatával egyidejűleg felül kell vizsgálni. Amennyiben az indokolt, az eljárásrendet a Szabályzat módosításával kapcsolatos eljárásrend szerint frissíteni kell.

111. Az adatátvitel sértetlensége, kriptográfiai eljárás

a) A Hivatal elektronikus információs rendszereivel kívülről kommunikáló minden rendszer esetén meg kell követelni olyan átviteli technológia meglétét, amely az adatátvitel sértetlenségét nem veszélyezteti, a továbbított adatok és információk bizalmasságát megvédi.

b) Az adatokat VPN csatornán keresztül és/vagy a megfelelő, szabványos vagy egyéb jogszabályokban biztonságosnak minősített **kriptográfiai eljárással** (legalább SSL/TSL réteg alkalmazásával) **titkosítani kell** az adatátvitel során az információk megváltozásának észlelésére.

c) Az elektronikus információs rendszerek kapcsolatát úgy kell megtervezni és kivitelezni, hogy az egy **munkaszakaszra épülő kétirányú** adatcsere befejezésekor, meghatározott időtartamú inaktivitás után a rendszer **megszakítja a kapcsolatot a külső rendszerrel.**

d) A meghatározott külső rendszerekkel történő kapcsolatra vonatkozó alkalmazott technológiákat az Infrastruktúra tervben részletesen szerepeltetni kell. Ugyanitt meg kell határozni az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges **kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó szabályokat is.**

e) Együttműködésen alapuló eszközök esetében az operációs rendszerben kell beállítani a **számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását,** kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

f) Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

112. Biztonságos név/cím feloldó szolgáltatások

a) Hivatal az informatikai hálózatában biztonságos név/cím feloldó szolgáltatásokat **(úgynevezett hiteles forrás)** használ.

b) Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi az utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) **hitelesíti az utód- és elődtartományok közötti bizalmi láncot.** (úgynevezett rekurzív vagy gyorsító tárat használó feloldás)

c) Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

d) Tartalékok, azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak **név/cím feloldási szolgáltatást** egy szervezet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

113. Rendszer karbantartási eljárásrend

a) A Hivatal elektronikus információs rendszereinek karbantartása, ütemezése a **jelen eljárásrend szerint történik.**

- A felhasználóknak az üzemeltetők felé kell jelezni:
  - a munka során tapasztalt és az elektronikus információs rendszerben fellépő hibákat, továbbá
  - az ellátandó egyéb üzemeltetői, ügyintézői feladatokat.

- Az üzemeltetők, amennyiben ismerik az egyszerű hibaelhárítás módszerét, akkor azonnali távsegítséget tudnak nyújtani a felhasználónak.

- Az üzemeltetők, ügyintézők kötelesek a hibát minél rövidebb időn belül kijavítani, elhárítani.

- A megoldott bejelentések adatai a Hivatal számára hiteles információt nyújtanak arra vonatkozóan, hogy az elektronikus információs rendszerben milyen hibák merültek fel, milyen további feladatokat kellett a működtetésük során ellátni,

- Az üzemeltetés során a szerver üzemeltetők figyelemmel kísérik az elektronikus információs rendszerek működtetéséhez alkalmazott rendszerelemeket, azok biztonsági frissítéseit, sérülékenységüket.

- A külső rendszerek esetén az adott szerződés szerint az üzemeltető, fejlesztő jelzi a telepítendő csomagokat, és azok kritikusságát.

b) priorizálás

A használt rendszerelemekhez kapcsolódó frissítések és sérülékenységek priorizálásra kerülnek aszerint, hogy mekkora kockázatot jelentenek a rendszer működésére és az adatbiztonságra, valamint aszerint, hogy a frissítés elvégzése okoz-e tartós rendszerleállást, illetve az milyen körben és arányban érinti a felhasználók munkavégzését.

c) rendszeres karbantartás

A rendszeres karbantartásokat az Informatika igény szerint, előre tervezett időtartamban végzi, úgy, hogy az esetleges nem várt események hatására hétfő munkakezdésig vissza lehessen állni a megelőző állapotra. A megelőző állapotot a beavatkozást megelőzően teljes körűen le kell menteni.

d) engedélyezés

A karbantartásokat és azok időtartamát a rendszerleállást kívánó időszakokra vonatkozóan a Jegyző engedélyezi.

Amennyiben a rendszer karbantartásához **külső szakértő beavatkozása** vagy közreműködése, **táv-support szolgáltatás igénybevétele** szükséges, úgy egy rendszer-beavatkozási kérelem (RBK) kitöltése szükséges a külső beavatkozó részéről. **A külső beavatkozást** az Üzemeltetési és Informatikai Csoportvezető engedélyezi.

e) Karbantartások, tervezett rendszerleállások kommunikálása

- A **tervezett rendszerleállások** időpontját és időtartamát (szükség esetén az okát, ha az nem

befolyásolja az információbiztonságot) a leállást megelőző 1 héttel korábban a publikus web oldalon az ügyfelek tájékoztatása érdekében és a belső portálon a munkavállalók, felhasználók tájékoztatására az információk között közzé kell tenni. Ha a leállás olyan rendszert érint, amelynek saját üzenő felülete is van, úgy a leállás időpontját és időtartamát ott is fel kell tüntetni.

- **A külső rendszerek karbantartásáról** szóló tájékoztatást – amennyiben az a hivatal működését érintheti – a külső rendszer karbantartójától kapott tájékoztatás alapján azonnal a publikus web oldalon az ügyfelek tájékoztatása érdekében és a belső portálon az információk között közzé kell tenni. Ha a leállás olyan rendszert érint, amelynek saját üzenő felülete is van, és azt az Informatika jogosult kezelni, úgy a leállás időpontját és időtartamát ott is fel kell tüntetni.

- A képviselői és /vagy bizottsági munkavégzést érintő leállásokról – függetlenül attól, hogy az külső vagy belső rendszert érint – a képviselőket, illetve a bizottsági tagokat az általuk meghatározott elektronikus levélcímen is értesíteni kell. Az értesítést a képviselők kapcsolattartói végzik az Informatika tájékoztatása alapján.

- Olyan karbantartási tevékenységek előtt, amelyek során más rendszerek, szolgáltatók rendszereinek működése befolyásolható, az érintett szervezeteket a tevékenység megkezdését megelőzően tájékoztatni kell úgy, hogy a beavatkozásra a szervezet fel tudjon készülni, az ügyfeleit megfelelő időben értesíteni tudja.

f) dokumentálás

Az elvégzett módosításokat dokumentálni kell, a változásokat az **Infrastruktúra Tervben illetve az Alkalmazás-katalógusban** át kell vezetni.

Az elszállított eszközöket a karbantartást követően a visszaszállításkor le kell ellenőrizni aszerint, hogy a visszaszállított eszközök javítása, karbantartása megtörtént-e, a javítás karbantartás elérte-e a célját, a javított eszközök megfelelően, biztonságosan működnek.

g) kritikus rendszerelemek

Hivatal a kritikus rendszerelemek vonatkozásában karbantartási támogatást, tartalék alkatrészeket szerez be a meghatározott elektronikus információs rendszerelemekhez.

h) felülvizsgálat

Jelen eljárásrendet legalább a Szabályzat felülvizsgálatával egyidejűleg felül kell vizsgálni.

114. Kritikus rendszerelemek

- Áramellátás
- Hálózati eszközök
- Háttértárolók
- Internet kapcsolat
- Külső és belső tűzfal rendszer
- Mentés
- Adatbázis-kezelő szoftver
- Szerverek
- Iratkezelő rendszer

115. Karbantartási eszközök és adathordozók ellenőrzése

a) Az informatikai rendszerüzemeltetők felelősek a munkájukkal összefüggő vagy rábízott beszerzések szakmai anyagának teljeskörűségéért, a leszállított eszközök, termékek ellenőrzéséért, tételes átvételéért.

b) Az Üzemeltetési és Informatikai Csoport vezetője a Beszerzési Szabályzat előírásainak megfelelően jár el a karbantartási eszközök mennyiségi és minőségi biztosítása érdekében.

c) A Hivatal Informatikai dolgozója minden karbantartást megelőzően akár külső, akár saját hatáskörben elvégzett karbantartás és javítás esetén átvizsgálja a karbantartási eszközöket biztonsági és adatbiztonsági szempontból.

d) Nem használható karbantartásra olyan eszköz, amely személyi sérülést okozhat, vagy nem elfogadható mértékű információbiztonsági kockázatot hordoz.

e) **Adathordozó ellenőrzés.** Azokat a karbantartási eszközöket, amelyek szoftverek tárolására és futtatására alkalmasak, ellenőrizni kell kártékony kódok, vagy nem megbízható hardverek vagy rendszerszoftverek vonatkozásában.

f) A kártékony kódot tartalmazó vagy gyanús eszközök nem csatlakoztathatók az információs rendszerelemekhez vagy a hálózathoz addig, amíg a veszélyt jelentő kódok megnyugtatóan nem kerültek eltávolításra az eszközről.

116. Távoli karbantartás

a) A Hivatal **a support szolgáltatási szerződések** megkötésekor gondoskodik arról, hogy elektronikus információs rendszerein távoli karbantartás csak előre egyeztetett időpontban, a megfelelő kommunikációs csatornán és porton, adott és azonosított távoli munkahelyről (IP cím) kizárólag a munkavégzéshez szükséges időtartamban és jogosultsággal, ellenőrzött körülmények között, jelen Szabályzatban meghatározott hitelesítést követően végezhet. Az előre definiált időtartamot, illetve ha a munkavégzés korábban befejeződik, a távoli kapcsolatot azonnali hatállyal bontani kell.

b) Távoli karbantartás kizárólag szerződéses jogviszonyban végezhető, a szerződésben a távoli karbantartásra vonatkozó kritériumokat definiálni kell. Csak olyan szervezet végezhet távoli karbantartást, aki
   - a szerződéses feltételek vonatkozásában a jelen Szabályzatban külső szolgáltatóra vonatkozó elvárásokat maradéktalanul elfogadta és teljesítette,
   - titoktartási nyilatkozatot tett minden résztvevője, így az általa távoli karbantartásra használt információs rendszere legalább a szervizelendő rendszerrel azonos biztonságú.

c) Amennyiben a karbantartáshoz használt rendszer nem biztonságos, úgy a szervizelendő elemet el kell távolítani az elektronikus információs rendszerből, és a távoli karbantartási és diagnosztikai szervizelést megelőzően minden információt törölni kell az érintett rendszerelemről.

117. Külső karbantartókkal kapcsolatos Eljárásrend

a) A Hivatal az elektronikus információs rendszereinek külső szolgáltatók által végzett karbantartási

eljárása jogszabályon és / vagy a szolgáltatóval kötött szerződésben definiáltak, valamint a jelen Szabályzatban meghatározott eljárásrend szerint történik.

b) Az információbiztonság biztosítása érdekében a fő szerződési előírások, védelmi szabályok a Hivatal részéről, a következők:

- A szerződéses ajánlatokban az ajánlattevőknek be kell nyújtaniuk a nemzeti vagyonról szóló 2011. évi CXCVI. törvény 3.§ (1) bekezdésében meghatározott ún. átláthatósági nyilatkozatot, megjelölve abban a vállalkozás tényleges tulajdonosát.

- A beszerzés tárgyától függően szerződéses, annak megerősítését szolgáló elem a Ptk. 6:159. § szerinti kellékszavatosság, a 6:160. § szerinti termékszavatosság, a 6:175. § szerinti jogszavatosság és a Ptk. 6:171. § szerinti jótállás előírása.

- A beszerzés tárgyától függően szerződéses elem a rendszeradaptálás, a beszerzéshez kapcsolódó rendszerkövetés.

- Szükséges szerződéses kötelem, ha a beszerzési tárgy rendelkezik ezzel, az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációi, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírása, a magas és alacsony szintű biztonsági tervek, - ha azzal a szállító rendelkezik - a forráskód és futtatókörnyezet beszállítói átadásának előírása; ha szükséges úgy a licenc jogosultság frissítésének beszerzése.

- Ha alkalmazásra kerül, akkor szállítói kötelezettség, a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereinek dokumentációja, a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához szükséges dokumentáció, a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját leíró dokumentáció, továbbá hogy az adminisztrátori és fejlesztői dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható, azt írásvédett elektronikus adathordozón adja át a szállító.

- Alkalmazandó szállítói kötelezettség, hogy a Hivatal érintett munkatársai számára elvégezze a szerepkörhöz tartozó jogosultságnak megfelelően a rendszerhasználati oktatásokat.

- A szerződések minőség ellenőrzés eredményét kizárólag a Polgármesteri Hivatal Üzemeltetési és Informatikai Csoportjának vezetője vagy a Hivatal vezetőjének döntése szerinti más személy igazolhatja le.

- A szerződés teljesítésében résztvevő szakemberek a helyszíni teljesítést / szolgáltatást a Polgármesteri Hivatal Informatikai Csoportjának vezetője vagy dolgozója jelenlétében végezhetik el.

- A szerződés teljesítésében résztvevő szakemberek / a szolgáltatást elvégző munkatársai külön-külön titoktartási kötelezettséget vállalnak, e célból készített nyilatkozat aláírásával.

- A szerződő fél a tudomásukra jutott minden nyilvánosság számára nem hozzáférhető információt bizalmasan kezel és kizárólag a másik Fél előzetes írásbeli hozzájárulásával hoz harmadik személy tudomására.

- A vállalkozó a teljesítés során betartja és végrehajtja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban Ibtv.), valamint a végrehajtására kiadott, a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és

biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben foglalt előírásokat, valamint a mindenkor hatályos a Megrendelő belső informatikai, adatvédelmi szabályzataiban rögzített és a szolgáltatást bármilyen módon befolyásoló, valamint a munkajogi, munkavédelmi szabályokat.

c) A karbantartásra jogosultak és a kapcsolattartók elérhetősége az **Informatikai Csoport Külsős vállalkozók jegyzéke** nevű dokumentumában kerülnek meghatározásra. A Hivatal iroda- és osztályvezetői kötelesek a külső karbantartókkal kapcsolatos együttműködésüket az Informatika felé haladéktalanul jelezni.

d) Karbantartási jogosultak azonosítása,

- Helyszíni karbantartási eljárás során az elektronikus információs rendszeren karbantartást végző szolgáltató delegáltjától meg kell követelni a hozzáférési jogosultság igazolását, a fizikai hozzáférés-védelmi fejezetben meghatározottak szerint a belépéseket adminisztrálni kell.

- Adott karbantartással összefüggésben kijelölt informatikai ügyintéző köteles a karbantartást végző személyeket és tevékenységeiket személyesen felügyelni.

e) Távoli hozzáférés szerinti beavatkozás nyilvántartása

A távoli hozzáférések során és a helyszínen végzett karbantartásokról az Informatika nyilvántartást vezet az RBK dokumentumok őrzésével.

118. Jogosultság-kezelési rend belső hálózatba történő külső (távoli) hozzáférésekhez

a) A Hivatal elektronikus információs rendszeréhez felhasználói hozzáférést engedélyezni kívülről kizárólag az elektronikus levelezéshez, Jegyző által jóváhagyott személyeknek szabad.

b) Tilos a levelezésen túl bármilyen külső felhasználói hozzáférést engedélyezni a belső rendszerekhez! Ettől eltérni nem lehet!

c) Az elektronikus postafiókhoz felhasználói hozzáférés kizárólag eszköz alapú, többtényezős hitelesítési eljáráson keresztül történhet.

d) A külső hozzáféréssel rendelkező munkatársakat a rendszer használatáról és a biztonsági kockázatokról, valamint azok kezeléséről dokumentáltan oktatni, képezni kell.

e) Hivatali alkalmazott karbantartás okán kívülről kizárólag többtényezős eszköz alapú hitelesítést követően kapcsolódhat a Hivatal belső, privilegizált elektronikus információs rendszereihez.

119. Külső munkatársak jogosultságainak kiadása

a) A külső munkatársat foglalkoztató szervezeti egység vezetője, Jegyzői engedéllyel, az Üzemeltetési és Informatikai Csoportvezetőt írásban értesíti a külső munkatárs számára a szükséges alap és felhasználói alkalmazás hozzáférés kiadásának engedélyezését.

b) A kérésnek tartalmaznia kell a **külső munkatárs és munkáltatójának a nevét, a kérés indokoltságát,**

valamint a jogosultság időtartamát.

c) Ilyen jogosultság kizárólag határozott időre adható meg. A határozott idő lejártakor a jogosultságokat azonnali hatállyal meg kell szüntetni.

d) A jogosultság nem hosszabbítható meg, szükség esetén azt újra kérvényezni kell.

e) Az engedélyeztetési folyamat során kedvezően elbírált jogosultság kizárólag a személy, személyes jelenlétű vagy ezzel egyenértékű (pl. a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott) tanúsítvány által történő azonosítása és hitelesítése útján adható ki.

f) A rendszerhez történő hozzáférést megelőzően a **külső munkatárssal alá kell íratni titoktartási** és a külső munkatársra vonatkozó kártérítési felelősség tudomásul vételéről valamint a releváns belső Szabályzatok megismeréséről és betartásáról és betartatásáról szóló **nyilatkozatot, valamint IT biztonsági oktatáson kell részt vennie.**

g) A külső munkatársak esetében a hozzáférési jogok kiadására és kezelésére ugyanazok a szabályok vonatkoznak, mint amik a Hivatal saját munkatársai esetén érvényben vannak.

120. Munkavégzés külső rendszereken, jogszabályban előírt feladatok ellátása

a) Külső rendszereken történő hivatali felhasználói munkavégzési típust, az ezzel kapcsolatos jogosítási kérelmet, jogosítási módosítást minden középvezető köteles a Jegyzőnek és az Üzemeltetési és Informatikai Csoportvezetőnek továbbítani.

b) A külső rendszerben történő munkavégzéshez a felhasználói jogosításokat az Informatika kijelölt munkatársa végzi a szakirodák által írásban igényelt és jóváhagyott jogosítási beállítások szerint.

c) Külső rendszereken történő munkavégzés csak a külső rendszer üzemeltetője Hivatallal kötött szerződésben és / vagy a külső üzemeltetői publikus feltételekben foglaltak szerint végezhető. Az engedélyezett külső rendszerek listáját az **Alkalmazáskatalógus tartalmazza.**

d) Külső rendszert használni csak a Jegyző engedélyével szabad. Az Informatika köteles meggyőződni arról, hogy a külső rendszer megfelel a Hivatal biztonsági előírásainak, és/vagy a jogszabályban kijelölt szerv által üzemeltetett rendszer biztonságáért a kijelölt szerv írásban vállalja a következményeket.

e) Külső rendszerbe nem nyilvános adatot bevinni csak hivatali felhatalmazás és jogszabályi kötelezettség alapján, csak a feldolgozandó ügyhöz szorosan kapcsolódó adatok vonatkozásában szabad.

f) A Hivatal elektronikus információs rendszerét külső rendszerrel összekapcsolni kizárólag megfelelő kockázatelemzési eljárást követően, az Informatikai biztonságért felelős személy engedélyével, jól definiált szerződés megkötésével vagy külső üzemeltetői feltételek mellett szabad.

g) A rendszerek összekapcsolásakor az Infrastruktúra tervben dokumentálni kell az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

XIII. Üzletmenet folytonosság tervezése, eljárásrend

1. A Hivatal külön dokumentumban: az Üzletmenet-folytonossági Terv, Szabályzatban (továbbiakban: BCP) megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül az érintett személyi kör részére kihirdeti az elektronikus információs rendszerre vonatkozó eljárásrendet, mely az üzletmenet-folytonosságra vonatkozó Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. Az üzletmenet-folytonossági tervben meghatározott gyakorisággal felülvizsgálja és frissíti az üzletmenet-folytonosságra vonatkozó eljárásrendet.

2. A Hivatal a külön dokumentumban (BCP) megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet.

3. A BCP terv meghatározza **az alapfeladatok (biztosítandó szolgáltatásokat) és alapfunkciók** kockázatgazdáját és a hivatali munkamegosztást, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket, rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről valamint definiálja a szervezet által előzetesen meghatározott alapszolgáltatások fenntartásának menetét, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is.

4. A BCP-ben meg kell határozni az elektronikus információs rendszer alapfunkcióit támogató kritikus rendszerelemeket is, valamint meg kell határozni, hogy az alapfunkciókat ellátó szervezeti egységek az üzletmenet-folytonossági terv aktiválását követőn **mennyi időn belül állíthatók fel.**

5. Munkamegosztás. A Hivatal összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével. Az üzletmenet-folytonossági tervet egyeztetni kell a kapcsolódó, hasonló tervekért felelős szervezeti egységekkel, pl. tűzvédelmi, munkavédelmi tervek elkészítéséért felelős szervezeti egység.

6. Az üzletmenet-folytonossági terv tesztelését megelőzően a kapcsolódó tervekért felelős szervezeti egységekkel egyeztetni kell. Az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket haladéktalanul tájékoztatni kell!

7. A BCP dokumentumban meghatározott gyakorisággal teszteli és felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet. A tesztelést követően kiértékelést végez. Az üzletmenet folytonossági tervet a tartalék feldolgozási helyszínen is tesztelni kell, hogy az érintett szervezet megismerje az adottságokat, és az elérhető erőforrásokat, valamint értékelje a tartalék feldolgozási helyszín képességeit a folyamatos működés támogatására.

8. Az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja, javítja az üzletmenet-folytonossági tervet, a javításokkal kapcsolatban az üzletmenet-folytonossági tervre vonatkozó általános eljárási szabályok szerint jár el.

9. A BCP megismerése. Az üzletmenet-folytonossági tervet tilos közzétenni vagy megismerhetővé tenni. Ez alól kivétel az olyan munkaköröket betöltő személyek, akihez a BCP-ben nevesítetten vagy munkakörüknél fogva feladat kerül hozzárendelésre.

10. Megismerheti továbbá az a vállalkozó, aki a kritikus folyamatok üzemeltetésében részt vesz, olyan mértékig, amennyire az üzletmenet folytonosság ezt indokolja. Ezek a személyek kötelesek titoktartási nyilatkozatot tenni a BCP-ben megismert adatok és információk kezelésére vonatkozóan.

11. A BCP dokumentumot nyomtatott formában, a Jegyző aláírásával hitelesítve az Informatikán lezárt, lepecsételt borítékban a fő és a tartalék helyszínen is zárt páncélszekrényben kell őrizni. Az üzletmenet-folytonossági intézkedések során csak ez a két példány tekinthető hitelesnek. A páncélszekrények kulcsát az Üzemeltetési és Informatikai Csoport vezetője és helyettese kezeli.

12. Üzletmenet-folytonossági képzés. A Hivatal az üzletmenet-folytonossága fenntartása érdekében a BCP dokumentumban meghatározott szerepkörrel rendelkező személyek és szervezeti egységek számára az üzletmenet-folytonossági terv változásakor, a kritikus folyamatokat támogató elektronikus információs rendszerben történő vagy a tervben meghatározott szerepkörökben történő személyi változások alkalmával a változásokat követő legfeljebb 3 hónapon belül felkészítő képzést szervez.

13. A felkészítő képzéseket változás hiányában legalább 3 évente meg kell tartani, a képzést a jelenlévőknek aláírásukkal igazolniuk kell.

14. Tartalék helyszín. A Hivatal az üzletmenet-folytonosság fenntartása érdekében az elsődleges helyszíntől különböző helyszínen, 1014 Budapest, Úri utca 58. szám alatti telephelyén elkülönített tartalék helyszínt, meleg tartalék helyszínt biztosít a feldolgozáshoz, a mentések és dokumentumok tárolásához, az elektronikus információs rendszerek infrastruktúrák, valamint szolgáltatások másodpéldányainak működtetéséhez.

    A Hivatal 1014 Budapest, Úri utca 58. szám alatti telephelyén biztosítani kell a BCP-ben rögzített minimális létszámú munkatárs munkavégzéséhez szükséges szobákat és helyiségeket.

15. Tartalék helyszínek inverz biztosítása egy esetleges katasztrófa helyzet esetére a következők:

    a) **a fő feldolgozási helyszín**: 1014 Budapest, Kapisztrán tér 1.

    b) **a tartalék feldolgozási helyszín:** 1014 Budapest, Úri utca 58.

XIV. Katasztrófaelhárítás tervezése, eljárásrendje

1. A Hivatal Üzletmenet-folytonossági Terv Szabályzata (továbbiakban: BCP, azaz Business Continuity Plan), annak részét képező **Katasztrófa-elhárítási Terv, Szabályzat (továbbiakban: DRP)** külön dokumentumként tartalmazza a teljes elektronikus információs rendszer helyreállításának tervét.

2. A folyamatot úgy kell meghatározni, hogy a helyreállítás során az eredetileg tervezett és megvalósított biztonsági védelmek és intézkedések intenzitása nem csökkenhet.

3. Hivatalban alkalmazott biztonsági eseménykezelési terv és eljárásrend az alábbiakban megfogalmazott, és dokumentált követelmények, struktúra és szervezet szerint az érintett személyek számára az Informatikai biztonságért felelős személy köteles megszervezni a DRP Terv Szabályzat tartalmára vonatkozó szakmai oktatást, legalább évente 1 alkalommal, továbbá a DRP Terv, Szabályzat változásakor, a kritikus folyamatokat támogató elektronikus információs rendszerben vagy azt kiszolgáló infrastruktúrában vagy meghatározott szerepkörökben történő személyi változások bekövetkezett változások esetén, legkésőbb az azt követő legfeljebb 3 hónapon belül **felkészítő képzést szervez.**

4. A DRP átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe, kielégíti az érintett szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit, meghatározza a bejelentésköteles biztonsági eseményeket az alábbiak szerint.

5. **A biztonsági események kezelése**

Biztonsági esemény bekövetkezésekor a szervezet minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről.
A PDCA elvet használjuk a folyamat leírására.

P - Plan
D - Do
C - Check
A - Act

- Megelőzés - Plan
- Észlelés, értesítés Do
- Reagálás, biztonsági esemény kezelése Check
- Kiértékelés Act

Megelőzés
humán megelőzési módszerek

- oktatás, tudatosítás

Alapvető és más lehetőségekhez képest olcsóbb módszer az, ha felkészítjük a felhasználókat, szervezet munkatársait arra, hogy felelősen, a biztonságot veszélyeztető tényezők ismeretében végezzék munkájukat. Továbbá legyenek felkészítve azoknak az eszközöknek és információs rendszereknek a használatára, amelyek szükségesek a munkájukhoz, így is csökkentve az emberi hibákból fakadó biztonsági eseményeket. Ennek eredményességét tudja fokozni, ha ezeket az ismereteket jól érthető formában, szakemberek által összeállított megbízható információkra építve adjuk át a dolgozóknak.

- műszaki személyzet képzése

A rendszereket üzemeltető és a biztonsági eseményeket első vonalban észlelő műszaki személyzet folyamatos képzése létfontosságú minden szervezet számára. Az „azonnal" kezelt biztonsági esemény nem eszkalálódik tovább, csökken annak a kockázata, hogy az adatok és jogosultságok sérüljenek, ezáltal csökkenjen a rendelkezésre állás.

- szimulációs gyakorlatok

A szervezet végezzen szimulációs gyakorlatot, hogy a kollégák fel tudjanak készülni az „éles" helyzetre, célszerű az „on the table" típusú gyakorlatok előtérbe helyezése a költséghatékonyság szem előtt tartása miatt.
műszaki megelőzési módszerek

- felhasználói gépek védelme

A közszférában dolgozó munkatársak a személyes tulajdonukban levő számítógépek tekintetében felelősek azok védelméért. Ez fokozottan fontos abban az esetben, ha ezeket a számítógépeket a hivatali kommunikációra, illetve munkavégzésre is igénybe veszik. Minden felhasználótól elvárható, hogy az alapvető védelmi intézkedések beállítását és működtetését képes legyen elvégezni. Ide soroljuk a rendszerszoftverek frissítését (Windows esetén például automatikusan elvégzi a rendszer, ha bekapcsoljuk), vírus és kártevő védelmi szoftverek működtetését (ingyenesen letölthetőek széles körű dokumentáció és telepítési utasítás áll rendelkezésre), és szoftveres tűzfal működtetését (Windows rendszer része, de ingyenes egyéb tűzfalak is elérhetőek).

- adatmentés

A legkézenfekvőbb megoldás, amely biztosítja az elektronikus információk megsemmisülés elleni védelmét az, ha többszörözzük őket. Le kell másolni rendszeresen, és az eredeti helyétől eltérő biztonságos helyen kell tárolni az információs rendszerekben és adathordozókon (külső merevlemez, DVD stb.) tárolt adatokat.

A másolatok megléte véd a rendszerek és adathordozók meghibásodása, a véletlen adattörlés vagy módosítás, és a szándékos károkozás ellen is. A másolásra alkalmazott műszaki megoldásoktól, az adatok visszaállítására használt eljárásoktól függ, hogy milyen gyorsan lehet visszaállítani az adatokat. A mentések gyakorisága pedig azt határozza meg, hogy két mentés között elvileg mennyi adat veszhet el.

Fontos felhívni a figyelmet, hogy adott szervezeten belül az informatikai részleg végzi az adatok mentését, ezért általában szükségtelen, sőt biztonsági szempontból kifejezetten veszélyes, gyakran tiltott is a munkavégzés során készített dokumentumok, iratok, levelezés saját adathordozón való tárolása, szervezeten kívülre hordozása.

- folyamatok, szolgáltatások folyamatos monitorozása

Minden szervezetnek szüksége van egy rendszerfelügyeleti szoftverre, ami képes a szervezet által üzemeltetett folyamatok és részfolyamatok folyamatos nyomon követésére, naplózható formában. Erre az ingyenesen használható NAGIOS rendszer teljesen alkalmas, telepítése üzemeltetése könnyen tanulható. felvehetők bele a szervezet elektronikus folyamatainak figyelése, riasztások állíthatók be vele.

- karbantartások elvégzése

A rendszeres karbantartás minden elektronikus információs rendszer és hardver rendszerelem vonatkozásában kiemelten fontos, hiszen csak ezeken keresztül lehet biztosítani a szervezet folyamatos működőképességet a nagy rendelkezésre állást.

- support szerződések

Lehetőség szerint, a szervezet alkalmazza a kockázatkezelés áthárítás funkcióját és kössön szerződést a beszállítókkal a kulcsfontosságú rendszerekre, level 2 szintű támogatásra. Ez az üzemeltetőknek is segítség, hiszen van hová fordulniuk, ha elakadnak egy probléma megoldásában.

Észlelés, értesítés

- automatikus észlelés

A beállított értékeknek megfelelően, különböző szintű riasztásokat küld az üzemeltetőknek a rendszerfelügyeleti szoftver, az előre megadott időpontokban.

- bejelentés e-mail

Az oktatáson tanultak és a begyakorlatokon példák alapján, a dolgozók felismerik és bejelentik az eseményt. A felhasználók az előre megadott e-mail címre továbbítják az észlelt eseménnyel

kapcsolatos információkat, lehetőség szerint képernyőképeket is. A bejelentés megtehető telefonon is, a biztonsági esemény típusától függően. A munkát fel kell függeszteni az adott rendszerben/hálózaton/számítógépen, amíg az üzemeltetők a biztonsági eseményt el nem hárítják.

Reagálás, biztonsági esemény kezelése

- cert értesítése

A törvényben rögzített esetekben kötelező a cert értesítése, ezzel egyidejűleg a Hivatal vezetésének értesítése is. A hálózatbiztonsági központok(certek), amelyeknek fő feladata a hálózatbiztonsági incidensek kezelése, az állami szféra vagy egyes ágazatok informatikai rendszereinek hálózatbiztonsági támogatása. A CERT-ek megfelelő technikai háttérrel rendelkeznek ahhoz, hogy időben reagáljanak és kezeljenek minden hálózatbiztonságra és létfontosságú információs infrastruktúrára veszélyes eseményt. A bejelentett eseményeket a központok bizalmasan vezetik.

- automatikus javítás

Ha az elektronikus információs rendszer képes rá, akkor végezze el az automatikus javítást(pl: adatbázis konzisztencia rendszeres ellenőrzése).

- helyi személyzet

A rendkívüli IT biztonsági esemény kivizsgálása általában helyben kezdődik. Meg kell nézni, hogy volt-e már hasonló eset, van-e elkerülő megoldás, illetve megoldás az IT biztonsági eseményre, illetve, hogy tényleg biztonsági esemény történik-e. A bejelentett eseményre a helyi üzemeltetés a szaktudásával próbáljon megoldást találni a lehető legrövidebb idő alatt, ha ez nem sikerül, akkor a support szerződés alapján tud külső segítséget kell igénybe venni.

- külső segítség

Bizonyos eseményeket a riasztó rendszerben, a külső partnerek felé kell automatikusan irányítani, hiszen Nekik lehet 24 órás ügyeletük, ami a Hivatalnak nem áll rendelkezésére. Így sokkal hamarabb értesülhetnek a területükhöz tartozó biztonsági eseményekről és hamarabb is tudnak reagálni rá.

Kiértékelés

Meg kell vizsgálni, hogy az intézkedések hatékonyak voltak-e, lehet-e jobban, gyorsabban reagálni hasonló esetben, hogyan lehet megelőzni hasonló biztonsági esemény bekövetkezését. Beépíteni a tervekbe, a tapasztalatokat és a szükséges erőforrásokat, valamint ennek megfelelően tartani a tudatosság képzéseket és vezetni a gyakorlatokat.

6. A biztonsági események dokumentálása

A biztonsági eseményeket folyamatosan nyomon kell követni és dokumentálni kell. Figyelni kell a tünetek ismétlődését, a hibajelenségeket össze kell vetni a korábban tapasztaltakkal. A Kockázatelemzési és -kezelési tervben meghatározott kockázatelemzési módszertannal meg kell határozni és ki kell értékelni a biztonsági esemény kockázatát, valamint meg kell határozni azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

Amint a Jegyző és / vagy az Információbiztonságért felelős személy tudomására jut a **személyes adatok kezelésével kapcsolatos** adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni köteles az illetékes felügyeleti hatóságnál, kivéve, ha az őt terhelő bizonyítási kötelezettség elvével összhangban igazolni tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes

személyek jogaira és szabadságaira nézve.

Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig - további indokolatlan késedelem nélkül - részletekben is közölni lehet.

7. **Biztonsági eseménykezelési terv megismerése.**
A biztonsági eseménykezelési terv csak az oktatáson során, a Hivatalban dolgozók számára ismerhető meg.

Gondoskodni kell arról, hogy a terv mások által ne legyen hozzáférhető, és módosítható.

8. **Biztonsági eseménykezelési terv változása**
A Biztonsági eseménykezelési terv változásakor a változásokat, valamint az új tervet és eljárásrendet meg kell ismertetni az érintett felhasználókkal, és a Szabályzatban történt változásokról, valamint jelen Szabályzat változásának megismeréséről és betartásáról minden érintettet nyilatkoztatni kell.

9. **Egyéb tevékenységek.** Az észlelt és kezelt eseményeket egyeztetni kell az üzletmenet-folytonossági tervhez tartozó tevékenységekkel, a levont tanulságokat be kell építeni az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe és tesztelésbe.

10. Kapcsolat a DRP és BCP tesztekkel. A feltárt és feltételezett biztonsági eseményeket az üzletmenet-folytonossági terv **tesztelési tervébe be kell építeni**, teszteléskor azzal egyidejűleg tesztelni kell. A beépített esetek tesztelését egyeztetni kell a kapcsolódó tervekben meghatározott szervezeti egységekkel és szerepkörökkel.

XV. Felhasználókra vonatkozó előírások

121. Személyi biztonsági Terv, viselkedési szabályok az interneten

A Szabályzat jelen fejezete foglalja össze azokat a felhasználók részére publikálható feltételeket, jogokat és kötelezettségeket, amelyek betartásával, figyelembe vételével a Szabályzat gyakorlati alkalmazása és az információ biztonság hatékonyan megvalósítható.

122. Felcsatlakozás

A hivatali hálózatba kapcsolt eszközökön az Internethez csak a Hivatal belső hálózatán keresztül szabad csatlakozni – szigorúan tilos bármilyen egyedi modem vagy vezeték nélküli internetes vagy más hálózati adatkommunikációra alkalmas megoldás használata.

123. Internet használata

a) A hivatali felhasználók a hivatali hálózatba kapcsolt eszközökön, valamint a hivatali eszközökön az Internetet csak a munkájukkal összefüggésben használhatják. Ettől eltérni nem lehet.

b) Az Internetet hivatali számítógépről vagy rendszerről kizárólag a Hivatal által biztosított internet kapcsolaton keresztül szabad használni.

c) Internethasználatra kizárólag azoknak a személyeknek van joguk, akik erre jogosultságot kaptak.

d) Az Internetet kizárólag a munkavégzéshez feltétlenül szükséges feladatokra és mértékig szabad használni.

e) Munkaidőben és munkaidőn kívül is tilos szabadidős tevékenységekre, programokra, hirdetésekre, reklámra, játékra, a felnőtt tartalmakra, közösségi hálózatra, internetes csevegésre, telefonálásra, fórumokra vonatkozó, a Hivatal jó hírnevét sértő, köztisztviselőhöz méltatlan vagy jogszabályba ütköző internetes alkalmazás használata vagy ilyen tartalom böngészése, letöltése, feltöltése, közzététele, küldése, fogadása.

f) Az Internet használatának alapelveit az Internetes illemtan, az **un. Netikett** (https://hu.wikipedia.org/wiki/Netikett) ide vonatkozó fejezetei fogalmazzák meg, amit minden felhasználónak kötelessége betartani.

g) Tilos az interneten fellelhető egyéb kockázatos alkalmazások használata (pl. prezi.com).

h) Hivatalban a nyilvánosan elérhető tartalom publikálására kizárólag az arra feljogosított informatikai ügyintézők, bizottsági titkárok és a közgyűlési előterjesztések, jegyzőkönyvek, indítványok kezelői meghatározott engedélyeztetési folyamatot követően jogosultak. A jogosult személyeket folyamatosan képezni kell annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne **tartalmazzanak nem nyilvános információkat.**

i) A publikált tartalmakat a Jegyző vagy az általa kijelölt személyek folyamatosan vizsgálják a publikálást megelőzően és követően, a feltárt hibákat javítják.

124. Letöltés

a) A hivatali munkavégzés és a közös üzemeltetés biztosítása érdekében kiemelt hivatali érdek a stabil internet sávszélesség biztosítása. Az Internetről tilos a munkához nem szükséges állományokat letölteni, vagy letöltött alkalmazást vagy szoftverkomponenst futtatni. pl. zenei és videomegosztó oldalak használata

b) Amennyiben az állományok letöltése a munkához elengedhetetlenül szükséges, a letöltött állományokra a megfelelő ellenőrzéseket (vírus- és kémprogram ellenőrzés) és védelmi intézkedéseket haladéktalanul el kell végezni.

c) Tilos az Internetről olyan állományok letöltése, amelyek letöltése vagy felhasználása jogszabályba ütközhet (például de nem kizárólag szerzői jogvédelem alatt álló állományok, futtatható állományok) és/vagy veszélyeztethetik az információbiztonságot. Az ilyen, ismert állományok letöltését a tűzfal beállításával is meg kell akadályozni.

125. Az elektronikus levelezéssel kapcsolatos magatartási szabályok

a) A Hivatal fontosnak tartja munkatársai hatékony belső és külső kommunikációját, ezért munkatársai számára elektronikus levelezési lehetőséget biztosít.

b) Az elektronikus levelezés célja a gyors ügyintézés és a papír alapú dokumentumok mennyiségének csökkentése.

c) A Hivatal minden munkatársától elvárja az elektronikus levelezéssel kapcsolatban a körültekintő és etikus viselkedést.

d) A Hivatal munkatársaira az alábbi, az elektronikus levelező rendszerre vonatkozó jogok és kötelezettségek vonatkoznak:

- a belső levelező rendszerben minden felhasználó egyedileg azonosítható;
- a munkatársak számára igényelhető elektronikus levélcím kötelező formátuma: vezeteknev.keresztnev@budavar.hu,
- ettől eltérni csak indokolt esetben, a Jegyző engedélyével lehet, valamint olyan esetekben amikor ez a formátum megtévesztő lehet (pl. két azonos nevű felhasználó esetén);
- a belső elektronikus levelező rendszerben továbbított üzenet, levél, vagy csatolt fájl egyenértékű az üzenet, levél, vagy csatolt fájl személyes, papír alapon történő átadásával,
- az elektronikus levelező rendszerből kifelé továbbított üzenet nem vonatkozhat kötelezettség vállalásra,
- az elektronikus levelező rendszerből kifelé továbbított bizalmas vagy szigorúan bizalmas üzenet csak nagyon indokolt esetben, csak titkosítva küldhető,
- az elektronikus levelező rendszerből kifelé továbbított levélben és üzenetben minden esetben biztosítani kell a Hivatal jó hírét,
- elektronikus levelezéskor az elektronikus levelezési címet csak az arra jogosult személy használhatja, más nevében elektronikus levél küldése nem engedélyezett, (kivéve a tisztségviselők kifejezett engedélyével a titkársági dolgozók esetét);
- az elektronikus levelező rendszer személyes célokra nem használható;
- a téves címzés miatt megkapott levelet bizalmasan kell kezelni, és azt haladéktalanul az eredeti címzettjének vagy a feladójának kell továbbítani, majd a levelezőrendszerből törölni kell

- a Hivatal elektronikus levelező rendszerében nem továbbítható zaklatást vagy más egyéb fenyegetést tartalmazó levél vagy üzenet, tilos a magáncélú, felnőtt témájú, jogszabályba ütköző tartalmak küldése, fogadása, megtárgyalása;
- tiltott tartalmú levél továbbításának az észlelését azonnal jelenteni kell az informatikai üzemeltetőknek és a szakiroda vezetőjének;
- a hivatali dolgozók munkavégzéshez csak a hivatali levelezőrendszert használhatják,
- nem használható és nem állítható be más szolgáltatótól vagy ingyenesen hozzáférhető levelező alkalmazás; ez alól kivétel a Belügyminisztérium által a polgármester és a jegyző számára hozzáférhetővé tett kormányzati levelezési rendszer (külön megállapodás szerint), valamint a választási informatikai rendszerben használt levelező rendszer;
- a Hivatalon belül tilos a lánc-levelek (ún. spam-levelek) pilótajáték-szerű továbbküldése, terjesztése.
- az Interneten továbbított üzenetek vagy levelek a Hivatalra vagy annak munkatársaira, ügyfeleire, szerződéses partnereire vonatkozó bizalmas vagy azok érdekeit sértő információt, politikai kijelentést, szitkot, vagy egyéb nyomdafestéket nem tűrő szöveget nem tartalmazhatnak.
- a Hivatal elektronikus levelező rendszerében az üzenetek és a levelek az Informatika által e célra létrehozott Hivatalos postaládákon keresztül kerülnek továbbításra;
- a postaládák tartalma a levelező rendszer mentése során kerül elmentésre.
- a hivatalban POP3 típusú levelezőszoftver használata tilos;
- ettől eltérni csak az Üzemeltetési és Informatikai Csoportvezető engedélyével szabad.;
- a helyi diszkeken tárolt levelekért az Informatikai Csoport nem vállal és nem vállalhat felelősséget, mivel azokon nem történik napi szintű mentés;
- a munkaállomásokon, informatikai eszközökön tilos SMTP szervert üzemeltetni,
- hivatalos vagy a hivatali munkával összefüggő elektronikus levelezést kizárólag a Hivatal által biztosított elektronikus levelezési cím és rendszer használatával szabad végezni;
- magán e-mail címek használata hivatalos levelezésre vagy a Hivatal rendszerein még ideiglenesen is tilos.

126. Adathordozókra vonatkozó kezelési, felhasználói eljárásrend

a) A felhasználók kötelesek az adathordozók használatával kapcsolatban a Szabályzatban előírt és az alábbiakban megismételt utasításokat betartani és betartatni.

b) Bármilyen **adathordozó használata a felhasználók számára tilos.**

c) Ettől eltérni csak a jelen Szabályzatban meghatározott feltételek teljesülése esetén szabad. Azon felhasználók, akik eltérő rendszerekhez is jogosultsággal rendelkezhetnek és a munkakörük alapján kötelesek külső harmadik személytől adathordozót átvenni; különös tekintettel a pályázatok, ajánlatok, műszaki tartalmú dokumentációk mobil adathordozón történő átvételi kötelezettségére, az Üzemeltetési és Informatikai Csoportvezető részére kötelesek írásban bejelenteni az adathordozó átvételt.

d) A felhasználó köteles az átvett eszközön a munkálatok megkezdése előtt egyedi vírusirtást kezdeményezni az informatikai üzemeltetőknél!

e) **Adatok biztonsága.** A felhasználó munkakör gyakorlása során lemezre (CD, DVD), vagy egyéb mobil tárolóra (pl. pendrive, flash disk, PDA, diktafon, fényképezőgép, mobiltelefon stb.) másolt adatok, dokumentumok bizalmasságáért, sértetlenségéért és rendelkezésre állásáért a másolatot készítő felhasználó fegyelmi felelősséggel tartozik.

f) A Hivatal megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek **tulajdonosa nem azonosítható.**

g) Az adathordozók biztonságos tárolását az adathordozó mibenlététől függetlenül, a tárolt adatok, dokumentumok bizalmasságának, sértetlenségének, rendelkezésre állási kötelezettségének és fontosságának megfelelően kell megoldani. Az adatok biztonságáért a másolatot készítő felhasználó fegyelmi felelősséggel tartozik!

h) **Adatmásolási tilalom.** Nem másolható adathordozóra olyan adat, amely személyes adatot vagy szigorúan bizalmas adatot tartalmaz.

i) Az adatmásolási tilalmat csak a Jegyző egyedi írásos felhatalmazása oldja fel, amelyben meg kell nevezni az adatok és az azokhoz hozzáférő felhasználók teljes körét, az adat adathordozón történő tárolásának végső határidejét, az adathordozóval kapcsolatos védelmi intézkedéseket, a felhasználás kizárólagos módját (módjait).

j) Adathordozók ellenőrzése. **Nem azonosított helyről származó adathordozók használata tilos.**

k) Adathordozók címkézése. Olyan adathordozókat, amelyek fizikailag nem kerülhetnek ki a Hivatal telephelyeiről meg kell jelölni az alábbi információkkal:
   - az adathordozón található adatok, információk köre
   - az adathordozón tárolt adatokhoz hozzáférők köre
   - az adatokra vonatkozó terjesztési korlátozások
   - az adathordozóra vonatkozó kezelési figyelmeztetések
   - megfelelő biztonsági jelzéseket

l) **Adathordozók védelme.** A címkézett adathordozókat minden esetben az Informatikán elzárt helyen és ellenőrzött módon kell tárolni.

m) A nem használt, fölöslegessé vált adathordozókat a jelen Szabályzatban meghatározottak szerint meg kell semmisíteni. A megsemmisítésig az adathordozókat elzárt helyen kell tartani az Informatikán.

n) **Adathordozók szállítása.** Az adathordozókat szállításkor – különösen a mentések tartalék telephelyre történő szállítása esetén – zárt páncélkazettában kell tárolni. A páncélkazetta egyik kulcsát a fő telephelyen, a másik kulcsát a tartalék telephelyen zárt helyiségben, páncélszekrényben kell tárolni. Szállítás közben a páncélkazetta kulcsa nem lehet a szállító személyzetnél.

o) Az adathordozókra vonatkozó eljárásrend tartalmának megismerését, a jelen Szabályzatban levő kötelezettségek felhasználókra és az informatikai üzemeltetőkre, ügyintézőkre vonatkozó részének megismertetése az Informatikai biztonságért felelős személy oktatás útján biztosítja.

p) A felhasználók, az informatikai üzemeltetők, ügyintézők a munkába állásukat megelőzően az informatikai jogosultságukra vonatkozó adatok átvételével együtt aláírásukkal dokumentálják az adathordozókra vonatkozó utasítások tudomásul vételét.

127. Felhasználók vírusvédelemmel kapcsolatos feladatai

a) Amennyiben a vírusellenőrzések ellenére a felhasználók vírusra utaló hibás, vagy furcsa működést tapasztalnak, a vírusfertőzés gyanújáról azonnal értesíteni kell az Informatikát.

b) A vírusdetektálás (vagy vírusgyanú felmerülése) és a víruseltávolítás biztonsági eseménynek számít, ezért minden vírusdetektálást és víruseltávolítást haladéktalanul jelenteni kell az Üzemeltetési és Informatikai Csoportvezető felé. Az ilyen eseményt az Informatikának k ki kell vizsgálnia, és az egyéb hibabejelentésekkel azonos módon dokumentálnia kell.

c) Amennyiben a vírusellenőrző rendszer fertőzést vagy fertőzésveszélyt jelez, az adathordozóról el kell távolítani a fertőzést vagy a veszélyes állományokat. Ha ez nem lehetséges, az adathordozót haladéktalanul el kell távolítani a rendszerből és az Informatikát értesíteni kell a fertőzésveszélyről.

d) Az adathordozót tilos a továbbiakban bármilyen rendszerhez csatlakoztatni (kivéve az Informatika vírusirtó rendszerét) addig, amíg az Informatika a fertőzés eltávolításáról nem gondoskodott kielégítően.

128. Alkalmazások futtatása

a) **Tiltott alkalmazások**
A kliens számítógépekre kizárólag az Informatika kijelölt ügyintézője telepíthet alkalmazásokat. A vírusok terjedésének megelőzése érdekében a munkaállomásokon **tilos olyan magas kockázatú alkalmazások** futtatása, amelyek a vírusok terjedésében kiemelt szerepet játszhatnak (egyes levelező, üzenő rendszerek).

b) **Operációs rendszerek**
A kliens számítógépekre kizárólag az informatikai üzemeltetők telepíthetnek meghatározott operációs rendszert.

c) **Futtatható állományok.**
- A helyi lemezeken (kivéve az Alkalmazáskatalógusban meghatározott alkalmazások állományait), adathordozókon, valamint a hálózati könyvtárakban a felhasználó számára tilos futtatható állományt tartani.
- Felhasználói joggal a rendszerben semmilyen alkalmazást nem lehet telepíteni.
- Munkavégzéshez kizárólag az Informatika által biztosított alkalmazások használhatók.
- A kliens számítógépeken a felhasználók nem kaphatnak adminisztrátori jogokat.

d) **Futtatható állományok törlése**
Az adathordozókon és a hálózati könyvtárakban található, nem engedélyezett futtatható állományokat az üzemeltetők – az Üzemeltetési és Informatikai Csoportvezető, a felhasználó, valamint a felhasználó szervezeti vezetője egyidejű értesítése mellett – haladéktalanul törlik.

e) **Frissítések kezelése**
Amennyiben a felhasználó jogosult a kliens számítógépen az operációs rendszer és egyéb rendszerek frissítésére, úgy folyamatosan – legalább napi szinten – **köteles ellenőrizni és letölteni** a megfelelő biztonsági frissítéseket.

129. Végpontvédelmi rendszerek használata

a) Végpontvédelmi rendszerek telepítése, eltávolítása
A kliens számítógépekre kizárólag az Informatika kijelölt ügyintézője telepíthet végpontvédelmi alkalmazásokat. A vírusirtó alkalmazások cseréje, törlése, indítópultból történő eltávolítása, kikapcsolása, működésének

akadályozása vírusadatbázisok manipulálása (kivéve a támogatott frissítéseket) még ideiglenes jelleggel is szigorúan tilos!

b) frissítések kezelése
A végpontvédelmi rendszert központilag automatikusan frissíti az üzemeltetés.

c) adathordozók ellenőrzése
Amennyiben a felhasználó adathordozók használatára jogosult úgy minden esetben az adathordozó csatlakoztatásakor minden más cselekményt megelőzően köteles teljes körű vírusellenőrzést alkalmazni a cserélhető adathordozóra.

130. Tiltott cselekmények a felhasználó számára

a) Magánjellegű felhasználás
A Hivatalban tilos, a Hivatal számítógépein és informatikai eszközein magánjellegű és/vagy jogszabályba ütköző adatok, alkalmazások tárolása, készítése, reprodukálása, és az informatikai eszközök, az elektronikus levelezés és az internetböngészés magánjellegű felhasználása.

b) **Telepítések tiltása. Tilos** a felhasználó számára a rendszerekre vagy rendszerelemekre bármilyen szoftverterméket telepíteni. A Hivatalban az elektronikus információs rendszerekhez és fiókokhoz kiosztott jogosultságok munkaköri besoroláson alapulnak, ugyanabban a munkakörben dolgozó munkatársak ugyanolyan jogosultságokkal rendelkeznek. Ettől eltérni csak egyedi esetekben, az adott szakiroda vezetője és az Üzemeltetési és Informatikai Csoportvezető engedélyével, dokumentáltan lehetséges.

c) Felhasználó semmilyen szoftvert nem telepíthet, azt kizárólag a kijelölt informatikai ügyintéző végezheti el.

d) Eszközök használatának tiltása
Tilos a Hivatali eszközökhöz a Felhasználók által bármilyen hardver eszközt (adatkommunikációra, adattárolásra alkalmas vagy bármilyen hardver eszközt, például, de nem kizárólag: USB pendrive, mobil internet stick, bluetooth adapter, Wi-Fi adapter, stb.) csatlakoztatni, az eszközök konfigurációját vagy hardver komponenseit megváltoztatni, az eszközt megbontani.

e) Beállítások módosítása
Tilos a rendszerek vagy rendszerelemek paramétereinek, beállításainak bármilyen megváltoztatása, kikapcsolása (pl. rendszerfrissítések letöltése, vírusvédelmi rendszer működése, frissítése, stb.), a védelmi intézkedések megkerülése.

f) Munkaszakasz zárolása. Az informatikai üzemeltetők és a felhasználók kötelesek biztosítani, hogy a Hivatalban alkalmazott vagy alkalmazni kívánt elektronikus információs rendszer meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést, valamint megtartja-e a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

g) A munkaszakasz zárolásakor a képernyőn korábban látható információt, egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - kell eltakarni.

h) Munkaszakasz lezárása. Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

i) Az eszközök munkával kapcsolatos felhasználása az adatvédelmi szabályok és állásfoglalások betartásával folyamatosan ellenőrzésre kerülnek!

j) Jelszavak, azonosítók, hitelesítő eszközök kezelésére vonatkozó felhasználói korlátozások, előírások:

- Tilos a felhasználói jogosultságú jelszavak átadása, megismertetése másokkal.
- Tilos mások nevében, mások azonosítóit használva belépni vagy belépést engedélyezni a rendszerekbe.
- Tilos olyan cselekményeket végrehajtani, amely által a felhasználó jelszava kompromittálódhat.
- Tilos a jelszavakat az azonosításhoz szükséges egyéb információkkal együtt tárolni (pl. rendszer hozzáférési címe, azonosítók, stb).
- Felhasználó köteles jelen Szabályzatban meghatározott előírások szerint a jelszavait folyamatosan adott időközönként megváltoztatni.
- Felhasználó nem használhat olyan jelszavakat, amelyek könnyen kitalálhatók vagy más, nem hivatali rendszerekben is alkalmazásra kerültek Felhasználó által.
- Felhasználó a személyes bejelentkezéséhez fűződő jelszavakat köteles úgy őrizni, hogy azok más számára ne legyenek megismerhetők.
- A jelszót tilos a munkaállomás környékén írásban tárolni.
- Jelszót tilos úgy tárolni, hogy az a felhasználó belépéshez szükséges kódjaként azonosítható és felismerhető legyen, valamint tilos a bejelentkezéshez szükséges bármilyen adat (belépéshez szükséges azonosító, rendszer elérési címe, stb.) jelszóval együtt tárolása.
- Felhasználó felelős az általa használt azonosítókkal történt cselekményekért, akkor is, ha az a felhasználónak felróható okokból került kompromittálódásra.
- A jelszó kompromittálódását vagy annak gyanúját a Felhasználó köteles haladéktalanul, írásban az Informatika tudomására hozni, az intraneten közzétett elérhetőségeken.
- Ha Felhasználó rendelkezik hitelesítő eszközzel, köteles az eszköz megóvása érdekében minden tőle telhetőt megtenni.
- Az eszközöket tilos átadni vagy hozzáférhetővé tenni más személyek számára.
- Az eszközökre tilos ráírni vagy vele összefüggésben az azonosításhoz szükséges bármilyen információt tárolni (pl. azonosító nevet, jelszót, a rendszer nevét, a belépéshez, eléréshez szükséges adatokat, stb.)

h) Adatok kezelése. Tilos a hivatal adatait adathordozóra másolni, azokról képi vagy egyéb másolatot készítve elektronikus vagy más módon a Hivatalból kijuttatni, vagy arra illetéktelenek számára betekintést vagy adatmegismerést lehetővé tenni.

i) Protokollok, internet. Tilos az Informatika által nem engedélyezett protokollok, portok, eszközök, alkalmazások használata, tiltott, továbbá a nem biztonságos, gyanús, nem ismert internet oldalak látogatása.

131. Tárterülettel kapcsolatos felhasználói magatartási szabályok.

a) Tilos a hivatali munkavégzéssel kapcsolatos dokumentumokat a Hivatalon kívüli tárhelyeken, FTP szervereken, tárhely szolgáltatóknál (pl. google drive) vagy külső felhő (pl. Microsoft Cloud) szolgáltatásban tárolni.

b) Felhasználók kizárólag a munkavégzéshez feltétlenül szükséges és elengedhetetlenül elektronikus

formában tárolandó fájlokat menthetnek az elektronikus információs rendszerekbe, kizárólag a személyes vagy csoport számára engedélyezett mappákba.

c) A kliens számítógépek merevlemezére vagy **lokális tárhelyére töltött adatokról nem készül biztonsági mentés,** így a lokális tárolókon (c:\, d:\, e:\, meghajtók vagy a lokális fájlrendszer /home vagy /media könyvtárak) tárolt adatokért kizárólag a Felhasználó felel.

d) Tilos a dokumentumokat többszörözni, más felhasználók számára tárolás céljából átadni vagy megosztani.

132. A felhasználó hordozható, saját mobil informatikai eszközeivel kapcsolatos kötelezettségei és a betartandó magatartási szabályok

a) Nem hivatali eszközöket (különösen: mobil telefon, laptop, notebook, tablet, pendrive) tilos a Hivatali hálózatba és a hivatal eszközeire csatlakoztatni.

b) Tilos a saját mobil eszközökkel történő és a hivatali munkavégzéssel kapcsolatos adatok, személyes adatok kamerával, fénykép, továbbá hangfelvétellel való rögzítése, tárolása.

133. Hivatali tulajdonban levő hordozható informatikai eszközre vonatkozó felhasználói szabályok.

a) A személyi leltárba adott informatikai eszközök és/vagy hordozható eszközök átadás-átvételi jegyzőkönyvére rávezetésre kerül az eszközre telepített operációs rendszer megnevezése, verziószáma, amennyiben licence-elt rendszert tartalmaz, a felhasználói licence száma és azonosítója (kulcs) valamint a telepített szoftverek listája és amennyiben ezek között licence-köteles termék is telepítésre került, úgy a felhasználói licenc azonosítói.

b) Az átadott eszköz vagy a telepített szoftverek és komponensek önkényes megváltoztatásáért az átvevő teljes körű anyagi és erkölcsi, valamint adott esetben büntetőjogi felelősséget vállal.

c) Az Informatika köteles a hordozható eszközökkel kapcsolatban felmerült szabálysértéseket vagy büntetőjogi eseteket a Jegyző számára jelezni.

XVI. Képzések tervezése, szervezése

A Jegyző az Informatikai biztonságért felelős személyen keresztül gondoskodik a Hivatal informatikai védelmi intézkedéseivel kapcsolatos publikus, megismerendő szabályok megismerhetőségéről.

134. Hivatalon belüli általános információbiztonsági célú hírek elektronikus közzététele.

a) Az Informatika rendszeres tájékoztatást nyújt a felhasználóknak a biztonsággal kapcsolatos eseményekről, változásokról, veszélyekről, azok elhárítására tett javaslatokról.

b) A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által üzemeltetett Kormányzati

Eseménykezelő Központ által küldött figyelmeztetéseket és riasztásokat az Információbiztonsági felelős továbbítja az Informatikai Csoportvezetőnek, aki a belső honlapon, szűkített – a felhasználók számára is értelmezhető, elégséges információt tartalmazó – módon közzéteszi.

c) A tájékoztatás e-mail-ben, és az Intranet portálon lévő hirdetőfalon történik.

135. Hivatali dolgozók, felhasználók számára képzések szervezése, azok megtartása

a) A hivatali dolgozók informatikai és információs biztonság-tudatosságát és a szerepkörükre vonatkozó tipizálható eseménykezelési eljárásokat a képzési tervben meghatározott rendszerességgel biztonsági képzések szervezésével kell folyamatosan biztosítani.

b) A képzésért felelős személy megfogalmazza, és dokumentálja, valamint elfogadásra javasolja a Képzési Eljárásrendet, amely célirányosan illeszkedik a jelenlegi és jövőbeli hivatali célkitűzésekhez, figyelembe veszi az információ vagyoni értékét, a hivatali értékeket.

c) Az Informatika az üzemeltetési tapasztalatok alapján rendszeres képzést indít valamely a fizikai védelmi intézkedések betartásával, a tudatos számítógép használattal, az információ biztonsággal, az adatvédelmi incidensek megelőzésével kapcsolatos magatartási, használati, biztonsági ismeretek elsajátítására, bővítésére, felfrissítésére.

d) A képzés tartalmazza az érintett személyek felkészítését a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket, felelősségüket a rendszer egésze iránt.

e) Az Információbiztonságért felelős személy a Hivatal középvezetői részére IT katasztrófaelhárítási képzést tart, évente legalább egy alkalommal.

f) Informatikai biztonsági képzésen minden ügyintézőnek részt kell vennie évente legalább egy alkalommal, illetve amennyiben a jogi környezetben, az informatikai védelem területén, az elektronikus információs rendszer területén jelentős változás várható vagy következett be.

g) Amennyiben olyan mértékű biztonsági kockázat vagy változás történik az információs rendszerekkel összefüggésben, hogy az indokol soron kívüli képzést, akkor az Informatika értesíti a képzésért felelős szervezeti egységet, aki megszervezi a felmerült biztonsági eseménnyel kapcsolatos képzést minden érintett ügyintéző számára.

h) A képzésen történő részvételt és a jövőbeni esetleges jogsértő tevékenységért való felelősségre való felhívást, a felhasználók az Informatika által készített jelenléti ív kitöltetésével és aláírásával ismerik el.

i) Az új foglalkoztatott és a tartós távollétről visszatérő köztisztviselők és közterület-felügyelők részére a munkába lépés előtt, információ biztonsági oktatást kell tartani, a jövőbeni kötelezettségek minél jobb elsajátítása érdekében.

j) A Hivatal iroda- és osztályvezetői kötelesek az Információbiztonságért felelős személy részére jelezni, ha olyan helyzet, tényállás merül fel és / vagy olyan személyi magatartás tapasztalható, ami indokolttá teszi az egyéni vagy csoportos eseti jellegű információ biztonsági oktatást.

136. Informatikai munkatársak képzése

a) Az Információbiztonságért felelős személy, az Informatika munkatársainak a felkészültségüknek megfelelő, a munkakörükkel összhangban levő információ biztonsági oktatást tart.

b) Az Informatika munkatársai kötelesek elősegíteni az információ biztonság fenntartását, meglevő és új kockázati tényezők esetén jelzéssel, elhárítási javaslattal élni.

c) Az informatikai konferenciákon, vagy szakmai tanulmányúton való részvétel – épp úgy, mint a társszervezetnél lévő tanfolyam vagy konzultáció – a képzés szerves részét képezi.

d) Az informatikai munkatársak kötelesek folyamatosan figyelemmel kísérni a felügyeleti hatóságok - NEIH és a GovCert – honlapjait, az ott publikált ismereteket a munkájuk során alkalmazni.

137. Szállítók, szolgáltatók részére történő oktatás.

a) Az elektronikus információs elem (hardver, szoftver, rendszer, stb.) beszerzésekor szerződésben indokolt esetben szerepel információ biztonsági oktatási ismeretekben részesítik az üzemeltetők a szállító, szolgáltató helyszíni képviselőit.

b) A Hivatalnak biztosítania kell olyan Szerződő Fél szolgáltatását, aki az elektronikai vagyonvédelmi rendszert tervező és szerelő feladatokat folyamatos ellátja. A Szerződő Fél alkalmazottja és / vagy alvállalkozója köteles részt venni a Hivatal képviselője által tartott információ biztonsági oktatáson, továbbá vállalkozói résztvevői titoktartási kötelezettséget vállalnak.

138. Szerepkör vagy feladat alapú biztonsági képzés.

A hivatali szervezeti egység vezetője köteles a szerepkör, vagy feladat alapú biztonsági képzés igényét az Üzemeltetési és Informatikai Csoportvezetőnek jelezni, a felhasználónak az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a neki kijelölt feladat végrehajtását megelőzően.

XVII. Hatálybalépés.

Jelen Szabályzat 2024. április 18. napján lép hatályba, egyidejűleg a Budapest Főváros I. kerület Budavári Polgármesteri Hivatal jegyzőjének az Informatikai Biztonsági Szabályzatról szóló 42/2022. (XII. 21.) számú utasítása hatályát veszti.

Budapest, 2024. április 15.

Czukkerné Dr. Pintér Erzsébet
jegyző

Budapest Főváros I. ker. Budavári Polgármesteri Hivatal Jegyző