Sárbogárdi Polgármesteri Hivatal

…3… / 2025.

SÁRBOGÁRDI POLGÁRMESTERI HIVATAL

Információbiztonsági Szabályzata

Jóváhagyom!

2025. október 1.

……

Dr. Venicz Anita Éva

címzetes főjegyző

Sárbogárd Város Jegyzője * 1. *

Verzió	Dátum	Módosította/létrehozta	Módosítás
0.1	2025. szeptember 28.	/Misák István	Létrehozás

Sárbogárd, 2025.

TARTALOMJEGYZÉK

I. ÁLTALÁNOS RÉSZ

I.1. AZ IBSZ CÉLJA

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) biztonságkezelési elveket, követelményeket és szabályokat tartalmaz a Sárbogárdi Polgármesteri Hivatal (továbbiakban: a Hivatal) tevékenykedő személyek (bizonyos feltételek esetén külső közreműködők) számára, akik felelősek az információbiztonság fejlesztéséért, megvalósításáért és megtartásáért. Az IBSZ hatékonyan támogatja a Hivatal biztonságkezelésének mindennapi gyakorlatát, illetve megfelelő kereteket biztosít a Hivatal teljes körű biztonsági szabályozásához.

Az IBSZ-ben szereplő követelményeket és rendelkezéseket a hatályos jogszabályok keretei között kell használni. A biztonsági szabályozás célja a következő:

a) A jogkövető magatartás és a jó hírnév érdekében védeni a szervezet értékeit;

b) A tudatosság, a szervezettség, a hatékonyság és a technikai megoldások használata segítségével növelni az információbiztonságot;

c) A megelőzés, a tájékoztatás, az oktatás, a felderítés és a szankcionálás eszközeivel segíteni az intézkedések érvényesítését.

A jelen IBSZ a Hivatal szervezeti szintű információbiztonsági szabályozó rendszerének egyik alapvető eleme. Az IBSZ a hatályos jogszabályokkal, a Hivatal működési és ügyrendi előírásaival összhangban megteremti az elektronikus információs rendszerek (továbbiakban: EIR vagy elektronikus információs rendszer) és az azokban kezelt adatok kockázatokkal arányos biztonságát. Tartalmazza a Hivatal elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott minimum információbiztonsági követelményeket, továbbá meghatározza azokat az elvárásokat, kötelezettségeket és a felelősséget, amelyekre a biztonságos információellátás érdekében szükség van.

A Hivatal informatikai szolgáltatóival kötött szolgáltatási szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen IBSZ-szel.

I.2. HATÁLY

I.2.1. Szervezeti személyi hatály

Az IBSZ szervezeti hatálya a Hivatal valamennyi olyan szervezeti egységére kiterjed, amely a Hivatal elektronikus információs rendszereit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz.

Az IBSZ személyi hatálya kiterjed a Hivatallal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek a Hivatal elektronikus információs rendszereivel (használják, fejlesztik, telepítik, üzemeltetik, javítják stb.), így:

a) a közszolgálati jogviszony alapján foglalkoztatott munkatársakra;

b) a közalkalmazotti jogviszony alapján foglalkoztatott munkatársakra;

c) a munkaviszony alapján foglalkoztatott munkatársakra;

d) a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyekre;

e) más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyekre.

I.2.2. Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed a Hivatal adataival és adatainak kezelésével összefüggésben használt bármilyen, a Hivatal rendelkezésében álló adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes, a Hivatal rendelkezésében álló[1] elektronikus információs rendszerre és ezek működési környezetére.

A tárgyi hatály kiterjed továbbá az ezen rendszerek működéséhez alkalmazott szoftverekre, illetve az ezekkel rögzített, tárolt, feldolgozott vagy továbbított adatokra és információkra.

I.2.3. Területi hatály

Az IBSZ területi hatálya a Hivatal székhelyére.

Az IBSZ területi hatálya kiterjed továbbá az összes információbiztonsági szempontból releváns helyiségére (egyéb létesítmények), illetve bizonyos feltételek mellett az elektronikus információs rendszerek szolgáltatóinak telephelyeire is.

I.2.4. Időbeni hatály

Jelen IBSZ a kiadás napján lép hatályba.

I.3. AZ IBSZ FELÜLVIZSGÁLATA

Az IBSZ eseti módosítására kerül sor, ha a benne szereplő adatok megváltoztak, illetve ha az IBSZ olyan kisebb mértékű kiegészítésekre szorul, amelyek nem érintik az aktuális biztonsági követelményeket.

Az IBSZ módosítására van szükség, ha a Hivatal elektronikus információs rendszereinek működésében vagy a Hivatal elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben jelentős változások következnek be.

Az IBSZ eseti felülvizsgálata és szükség szerinti módosítása a változást követő 60 napon belül kötelező.

Az IBSZ-t legalább évente egy alkalommal felül kell vizsgálni.

Az IBSZ eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az elektronikus információs rendszerek biztonságáért felelős személy (továbbiakban: információbiztonsági felelős, rövidítve IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a Jegyző hatásköre.

Amennyiben az éves felülvizsgálat eredményeképpen a szabályzat módosítására nincs szükség, abban az esetben a felülvizsgálat tényéről a felülvizsgálatért felelős személy feljegyzést készít, melyet az iktatott IBSZ mellé csatolni szükséges.

[1] Kibertv. 6.§ (1) bekezdése alapján

I.3.1. Hatásköri és illetékességi szabályok

Az IBSZ belső használatú dokumentum: a Hivatal elektronikus információs rendszerének felhasználói, illetve egyéb érintettek (a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyek, más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyek) megismerhetik és birtokolhatják, de illetékteleneknek nem adhatják tovább.

I.4. KAPCSOLÓDÓ DOKUMENTUMOK

I.4.1. Jogszabályok

a) AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2022. december 14-i (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

b) AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet);

c) AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről;

d) 2012. évi I. törvény a munka törvénykönyvéről;

e) 2018. évi CXXV. törvény a kormányzati igazgatásról;

f) 2012. évi C. törvény a Büntető Törvénykönyvről;

g) 2013. évi V. törvény a Polgári Törvénykönyvről;

h) 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól;

i) 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (továbbiakban: Kibertv.);

j) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Info tv.);

k) 2016. évi CL. törvény az általános közigazgatási rendtartásról;

l) 1999. évi LXXVI. törvény a szerzői jogról;

m) 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről (továbbiakban: Kszetv.)

n) 2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról (továbbiakban: Vbö.)

o) 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról (továbbiakban: Kiber vhr);

p) 146/1993. (X. 26.) Korm. rendelet a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtásáról;

q) 322/2024. (XI. 6.) Korm. rendelet a digitális szolgáltatások, a digitális állampolgárság szolgáltatások és támogató szolgáltatások részletes műszaki követelményeiről;

r) 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről (továbbiakban: technológiai vhr);

s) 17/2025. (VII. 24.) EM rendelet a Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelményekről.

I.4.2. Kapcsolódó szabványok, ajánlások

a) MSZ EN ISO/IEC 27002:2023: Információbiztonság, kiberbiztonság és a magánélet védelme. Információbiztonsági kontrollok/intézkedések (ISO/IEC 27002:2022)

b) MSZ ISO/IEC 27001:2022/Amd 1:2024: Információbiztonság, kiberbiztonság és a magánélet védelme. Információbiztonság-irányítási rendszerek. Követelmények. 1. módosítás: Az éghajlatváltozás elleni fellépést célzó intézkedések;

c) NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations;

d) NIST Special Publication 800-53A Revision 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations;

e) NIST Special Publication 800-55 Performance Measurement Guide for Information Security;

f) NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization;

g) NIST SP 800-18 Rev. 1 Guide for Developing Security Plans for Federal Information Systems;

h) NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management

i) NIST 800-88 Rev1 - Guidelines for Media Sanitization.

j) Open Web Application Security Project Testing Guide aktuális verziója;

k) Open Web Application Security Project Application Security Verification Standard (ASVS) aktuális verziója;

l) Open Web Application Security Project Mobile Security Testing Guide aktuális verziója;

m) Open Web Application Security Project Mobile Application Security Verification Standard aktuális verziója;

n) Open Web Application Security Project Password Storage Cheat Sheet.

I.4.3. Az IBSZ-hez kapcsolódó belső dokumentumok

a) Szervezeti és Működési Szabályzat;
b) Adatvédelmi és Adatbiztonsági Szabályzat;
c) Iratkezelési Szabályzat;
d) Selejtezési Szabályzat;
e) Információbiztonsági kockázatelemzés.

I.5. AZ IBSZ ÁLTALÁNOS KÖVETELMÉNYEI

Az IBSZ és a jelen IBSZ *{4. számú melléklet – Felhasználói Informatikai Biztonsági Házirend}* melléklete (továbbiakban: FIBH) előírásainak alkalmazása, betartása, illetve betartatása, a *{I.2.1. Szervezeti személyi hatály}* pontban megjelöltek számára kötelező.

Az információbiztonsági előírások betartása megvédi a Hivatalt és a *{I.2.1. Szervezeti személyi hatály}* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan, vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

Titoktartási kötelezettség terhel minden, a Hivatal informatikai rendszereivel kapcsolatba kerülő természetes és jogi személyt, tekintet nélkül arra, hogy a kapcsolat milyen jogviszonyból ered. A titoktartási kötelezettség a szerződéses partnerek alvállalkozóira teljes körűen vonatkozik.

A titoktartási kötelezettség kiterjed a rendszerben kezelt adatokra, valamint a rendszer felépítésére, működési rendjére vonatkozó adatokra, a biztonsági rendszabályokra egyaránt. A titoktartási kötelezettség időkorlát nélkül áll fenn és az érintett személy a mindenkor érvényes jogszabályok alapján tartozik ezen kötelezettségéért felelősséggel.

Minden munkatárs (beleértve az ideiglenes, ill. megbízási szerződés alapján munkát végző munkatársakat is) csak Titoktartási nyilatkozat aláírása után kezdheti meg az érdemi munkát, kaphat hozzáférést információkhoz, erőforrásokhoz.

A felhasználók részére a FIBH tartalmaz egy kivonatot, melynek megismeréséről és betartásáról írásban nyilatkozniuk kell.

A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. Az IBSZ és a FIBH el nem olvasása, vagy nem ismerete nem mentesít a felelősség alól.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák a FIBH előírásait.

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ *{6. számú melléklet – Felhasználói Nyilatkozat}* mellékletében található nyilatkozat aláírása után lehet használatba venni.

A jelen IBSZ a Kibertv. 6. § (10) bekezdése alapján a technológiai vhr ALAP biztonságára előírt követelményeket tartalmazza. A Kibertv. 85. §-a alapján, a csillaggal megjelölt fejezetek 2026. január 1-jén hatályosulnak.

A Kibertv. 6.§ (10) bekezdése alapján a Hivatalnak

a) nem kell teljes körű kockázatmenedzsment keretrendszert működtetni;

b) nem kell hatáselemzést és kockázatmenedzsment tevékenységet végeznie

c) nem kell elvégeznie az elektronikus információs rendszerben kezelt adatok felmérését és osztályozását;

d) nem kell értékelnie az informatikáért felelős miniszter rendelete szerint kiválasztott védelmi intézkedések megfelelőségét;

e) nem kell értékelnie a védelmi intézkedéseket.

II. VÉDELMI INTÉZKEDÉSEK

II.1. PROGRAMMENEDZSMENT

A technológiai vhr **PROGRAMMENEDZSMENT** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.1.1. Információbiztonsági szabályzat

A Hivatal Információbiztonsági szabályzatát a jelen dokumentum tartalmazza.

II.1.2. Elektronikus információs rendszerek biztonságáért felelős személy

A Hivatalnak meg kell bíznia vagy ki kell jelölnie az elektronikus információs rendszerek biztonságáért felelős személyt (továbbiakban: IBF).

Az IBF feladat, hatás és felelősségi körét a jelen IBSZ *{II.2.1.2.Az IBF}* pontja tartalmazza.

II.1.3. Információbiztonságot érintő erőforrások

Az éves költségvetési tervezési folyamatban ki kell térni az elektronikus információs rendszerek biztonsági beruházásainak tervezésére oly módon, hogy a Hivatal költségvetésében elkülönítetten szerepeljen.

A biztonsági beruházások tervezését az informatikai biztonsági stratégiai célok, valamint a cselekvési tervekben megfogalmazottak alapján kell elkészíteni.

A tervezési dokumentumot az informatikai területért felelős vezető készíti el az információbiztonsági felelőssel együttműködve.

A tervezési dokumentumban legalább a következőket kell feltüntetni:

a) beruházás megnevezése;

b) beruházás indoka, célja, kezelt kockázat;

c) költség-haszon elemzés;

d) a beruházás elhagyásának következményei (jogi, információbiztonsági kockázat).

Az információbiztonsági beruházások tervezését tartalmazó előterjesztést – az informatikai beruházások tervezésével együtt – az informatikáért felelős szervezeti egység vezetője terjeszti be a Jegyző részére jóváhagyás céljából.

II.1.4. Intézkedési terv és mérföldkövei

A Hivatal bevezet egy folyamatot, amely biztosítja, hogy az információbiztonság és az ellátási lánc kockázatkezelése, valamint a kapcsolódó szervezeti elektronikus információs rendszerek (a továbbiakban: EIR-ek) intézkedési tervei:

a) ki legyenek dolgozva és karban legyenek tartva;

b) dokumentálják a helyreállító információbiztonsági és ellátási lánc kockázatkezelési intézkedéseket, hogy megfelelően reagáljanak a szervezeti műveletek eszközök, személyek és más szervezetek kockázataira;

c) a meghatározott jelentési követelmények bemutatásra kerüljenek.

2 évente felül kell vizsgálni az intézkedési terveket és mérföldköveket, hogy azok összhangban állnak-e a szervezeti kockázatmenedzsment stratégiával és a kockázatkezelési intézkedések szervezeti szintű prioritásaival.

II.1.5. Elektronikus információs rendszerek nyilvántartása

Nyilvántartást kell vezetni a Hivatal által működtetett valamennyi elektronikus információs rendszerről. A nyilvántartásnak minden elektronikus információs rendszerre nézve a következőket kell tartalmaznia:

d) az EIR nevét;

e) annak alapfeladatait;

f) biztonsági osztályba sorolását;

g) a rendszerek által biztosítandó szolgáltatásokat;

h) az érintett rendszerekhez tartozó licenc számot;

i) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;

j) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

A nyilvántartást a rendszergazdának kell vezetnie és évente felülvizsgálnia.

II.1.6. A biztonsági teljesítmény mérése (*)

A Hivatal a *{NIST Special Publication 800-55 Performance Measurement Guide for Information Security}* dokumentumban található mérőszámok alapján az elektronikus információs rendszerei biztonsági teljesítményének a mérését következők szerint végzi.

A méréseket az IBF-nek kell elvégeznie a biztonságértékelési terv végrehajtásával párhuzamosan. A mérések eredményéről az IBF tájékoztatja a Jegyzőt, a szükséges beavatkozásokat (eljárásrendek módosítása, felhasználói tesztek javítása) az IBF végzi el.

II.1.6.1. Szabálysértések száma

Mérni kell, hogy hányszor és milyen okból kellett eltérni az információbiztonságra vonatkozó szabályzatokban, eljárásrendekben foglaltaktól.

a) Mérőszám neve: Szabálysértések száma;

b) Mérés célja: Megbizonyosodni arról, hogy hányszor és milyen okból kellett eltérni az információbiztonságra vonatkozó szabályzatokban, eljárásrendekben foglaltaktól, illetve hányszor sérült a szabályokban foglaltak végrehajtása;

c) Mérőszám leírása: Az adott évben a szabálytól való eltérések száma;

d) Sikerkritérium: évente 5-nél kevesebb;

e) Mérés gyakorisága: évente;

f) Mérési adat forrása: Biztonsági incidensek jegyzőkönyvei.

II.1.6.2. Biztonsági incidensek száma

Mérni kell, hogy egy adott időszakra vonatkozóan hány biztonsági esemény történt az elektronikus információs rendszerek működése során.

a) Mérőszám neve: Biztonsági incidensek száma;

b) Mérés célja: Megbizonyosodni a biztonsági incidensek számáról;

c) Mérőszám leírása: Az adott évben a biztonsági incidensek száma;

d) Sikerkritérium: 2 db;

e) Mérés gyakorisága: Évente;

f) Mérési adat forrása: Biztonsági incidensek jegyzőkönyvei.

II.1.6.3. SLA

Mérni kell, hogy az elektronikus információs rendszerek nyilvánosan elérhető elemei (partnerek, ügyfelek részére biztosított) hány alkalommal nem voltak elérhetőek és össze kell vetni az ÜFT-kben vállalt rendelkezésre állási mutatókkal.

a) Mérőszám neve: SLA;

b) Mérés célja: Megbizonyosodni arról, hogy a vállalt SLA érték teljesült-e;

c) Mérőszám leírása: X=(vállalt szolgáltatási időszak-kiesési idő órában)/szolgáltatási időszak*100;

d) Sikerkritérium: <99,9%;

e) Mérés gyakorisága: évente;

f) Mérési adat forrása: Internetszolgáltatótól beszerzett statisztika, web szerver és a tűzfal naplói.

II.1.6.4. Alkalmazás hibáinak a száma

Mérni kell, hogy az elektronikus információs rendszerek működése során hány hibát nem sikerült elhárítani.

a) Mérőszám neve: Alkalmazás hibák;

b) Mérés célja: Megbizonyosodni arról, hogy kellő hatékonysággal kezelik-e a felhasználók által bejelentett hibákat;

c) Mérőszám leírása: X=(összes hiba-kezeletlen hiba)/összes hiba*100;

d) Sikerkritérium: 99%;

e) Mérés gyakorisága: évente;

f) Mérési adat forrása: Hibajegyek.

II.1.6.5. Biztonságtudatossági képzés

Mérni kell a biztonságtudatossági képzésen résztvevő felhasználók számát, illetve a kitöltött teszt sikerességét.

a) Mérőszám neve: Biztonságtudatossági képzés;

b) Mérés célja: Megbizonyosodni arról, hogy kellő hatékonysággal sajátítják el a képzési anyagot a felhasználók;

c) Mérőszám leírása: (összes felhasználó szám-tesztet nem teljesítők)/összes felhasználó száma*100;

d) Sikerkritérium: 99,5%;

e) Mérés gyakorisága: évente;

f) Mérési adat forrása: Felhasználói tesztek.

II.1.6.6. Szerepkör alapú képzés

Mérni kell a szerepkör alapú biztonságtudatossági képzésen részt vevő felhasználók számát, illetve a kitöltött teszt sikerességét.

a) Mérőszám neve: Szerepkör alapú képzés;

b) Mérés célja: Megbizonyosodni arról, hogy kellő hatékonysággal sajátítják el a képzési anyagot a felhasználók;

c) Mérőszám leírása: (Szerepkör alapú képzéseken részt vevők – sikertelen vizsgázók száma)/ Szerepkör alapú képzéseken részt vevők *100;

d) Sikerkritérium: 99,5%;

e) Mérés gyakorisága: évente;

f) Mérési adat forrása: Szerepkör alapú tesztek.

II.1.6.7. ÜFT tesztelése

Mérni kell az ÜFT-k tesztelését.

a) Mérőszám neve: ÜFT teszt;

b) Mérés célja: Megbizonyosodni arról, hogy kellő hatékonysággal tesztelik-e a kidolgozott ÜFT-ket;

c) Mérőszám leírása: (végrehajtott tesztek száma - sikertelen tesztek száma)/végrehajtott tesztek száma*100;

d) Sikerkritérium: 99,5%;

e) Mérés gyakorisága: évente;

f) Mérési adat forrása: Szerepkör alapú tesztek

II.1.6.8. Előírt dokumentációk elérhetősége

Meg kell vizsgálni, hogy az egyes EIR-ek megfelelően dokumentáltak-e.

a) Mérőszám neve: EIR dokumentációk;

b) Mérés célja: Megbizonyosodni arról, hogy az EIR-ek rendelkeznek-e az előírt dokumentációkkal;

c) Mérőszám leírása: (Megfelelő dokumentációval rendelkező EIR-ek száma/összes EIR száma*100;

d) Sikerkritérium: 100%;

e) Mérés gyakorisága: évente;

f) Mérési adat forrása: Informatikai Osztály által szolgáltatott információk.

II.1.6.9. Sérülékenységek száma

Mérni kell az egyes EIR-ekben felfedezett és nem kezelt magas vagy kritikus sérülékenységek számát. A mérést EIR-enként kell elvégezni.

a) Mérőszám neve: EIR sérülékenységek;

b) Mérés célja: Megbizonyosodni arról, hogy az EIR-ek rendelkeznek-e publikus magas vagy kritikus sérülékenységgel;

c) Mérőszám leírása: (Adott időszakban az EIR-ben felfedezett magas vagy kritikus sérülékenységek száma/Adott időszakban kezelt magas vagy kritikus sérülékenységek száma)*100;

d) Sikerkritérium: 100%;

e) Mérés gyakorisága: évente;

f) Mérési adat forrása: Sérülékenység vizsgálatok jegyzőkönyvei.

II.1.6.10. Mobil eszközök biztonsága

Meg kell bizonyosodni arról, hogy a Hivatal adatokat kezelő mobil eszközök közül hány eszközön alkalmaznak megfelelő tároló titkosítást.

a) Mérőszám neve: Mobil eszközök biztonsága;

b) Mérés célja: Megbizonyosodni arról, hogy Hivatal adatokat kezelő mobil eszközök közül hány eszközön alkalmaznak megfelelő tároló titkosítást;

c) Mérőszám leírása: (tároló titkosítást alkalmazó Hivatal adatot kezelő mobil eszköz/összes Hivatal adatot kezelő mobil eszköz)*100;

d) Sikerkritérium: 100%;

e) Mérés gyakorisága: évente;

f) Mérési adat forrása: Vagyonleltár.

II.1.7. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve (*)

A Hivatal a Hivatal működése szempontjából kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági tervének kidolgozása, dokumentálása és frissítése során kezeli az információbiztonsági kérdéseket.

Ennek érdekében a fenti területek tervezése és működtetése során felmerülő információbiztonsági kérdéseket véleményeztetni kell az IBF-fel.

II.1.8. Kockázatmenedzsment stratégia (*)

A Hivatalnak a Kibertv. 6.§ (10) bekezdése értelmében nem kell kockázatmenedzsment keretrendszert, illetve hatáselemzést és kockázatmenedzsment tevékenységet végeznie.

II.1.9. Engedélyezési folyamatok meghatározása

A Hivatalnak az IBSZ-ben meghatározott engedélyezési folyamatokon keresztül kell kezelnie az EIR-ek és azok környezetének biztonsági állapotát.

A szervezet kockázatmenedzsment folyamatának felelőseit (névvel és felelősségi körrel ellátva) a jelen IBSZ *{II.1.11. Szervezeti működés és üzleti folyamatok meghatározása}* és kockázatkezelés fejezetei tartalmazzák.

II.1.10. Az információbiztonsági felelősségi rend meghatározása

Az engedélyezési folyamatokat be kell illeszteni a Hivatal egészét átfogó kockázatmenedzsment keretrendszerbe.

II.1.11. Szervezeti működés és üzleti folyamatok meghatározása (*)

A Hivatalnak meg kell határoznia a szervezeti célokat és az üzleti folyamatokat, figyelembe véve az információbiztonságot, valamint a szervezeti működésre, eszközökre, személyekre és más szervezetekre gyakorolt kockázatokat.

Meg kell határozni továbbá a szervezeti célokból és üzleti folyamatokból adódó információvédelmi igényeket.

Meghatározott gyakorisággal felülvizsgálja és módosítja a szervezeti célokat és az üzleti folyamatokat.

A Hivatalnak rendes felülvizsgálat keretein belül 3 évente felül kell vizsgálnia és frissíteni kell a stratégiát.

Amennyiben a Hivatal szervezetében lényeges változás történik, akkor soron kívül felül kell vizsgálnia a stratégiát.

A felülvizsgálatokban az IBF-et be kell vonni.

II.1.12. Biztonsági személyzet képzése (*)

A Hivatal a jogszabály által kijelölt szerv által megszervezett továbbképzésen és éves továbbképzésen biztosítja a részvételét a

a) Jegyzőnek;

b) az informatikai terület munkatársainak;

c) és az IBF-nek.

II.1.13. Tesztelés, képzés és felügyelet (*)

A Hivatalnak be kell vezetnie egy folyamatot, amely biztosítja, hogy a szervezeti EIR-ekhez kapcsolódó biztonsági tesztelések, képzések és felügyeleti tevékenységek elvégzésére vonatkozó szervezeti tervek megfelelő fejlesztés és karbantartás mellett folyamatosan végrehajtásra kerüljenek.

A Hivatalnak felül kell vizsgálnia és össze kell hangolnia a terveit a szervezeti kockázatmenedzsment stratégiával és a kockázatkezelési intézkedésekre vonatkozó, az egész szervezetre kiterjedő prioritásokkal.

II.1.14. Szakmai csoportokkal és közösségekkel való kapcsolattartás

Az IBF-nek nyomon kell követnie a Hatóság által közzétett riasztásokat és tájékoztatásokat és ezek alapján felhasználói körlevelek formájában is elő kell segítenie (az éves kötelező biztonságtudatossági képzésen túl) a felhasználók biztonságtudatosságának fenntartását. A megszerzett információkat be kell építeni az éves biztonságtudatossági képzés anyagaiba is.

Az EIR-ek üzemeltetésbiztonságának fenntartása érdekében az IBF nyomon követi és a munkája során felhasználja a nemzetközi mértékadó szervezetek (pl.: NIST, CIS, OWASP) szabványait, ajánlásait.

A Hivatalnak ki kell választania azokat a szakmai csoportokat és közösségeket, akikkel felveszi és kialakítja a kapcsolatot a kiválasztott annak érdekében, hogy

a) elősegítse a szervezethez köthető személyek folyamatos biztonsági oktatását és képzését;

b) naprakész információkkal rendelkezzen az ajánlott biztonsági gyakorlatok, technikák és technológiák terén;

c) megossza az aktuális biztonsággal kapcsolatos információkat, beleértve a fenyegetéseket, sérülékenységeket és biztonsági eseményeket.

II.1.15. Fenyegetettség tudatosító program (*)

Fenyegetettség tudatosító program követelményt a jelen IBSZ ***{Hiba! A hivatkozási forrás nem alálható.. Hiba! A hivatkozási forrás nem található.}*** a ***{Hiba! A hivatkozási forrás nem található.. Hiba! A hivatkozási forrás nem található.}*** és a ***{Hiba! A hivatkozási forrás nem található.. Hiba! A hivatkozási forrás nem található.}*** fejezetei tartalmazzák.

A Hivatalnak a fenyegetésekkel kapcsolatos információk megosztására fenyegetettség tudatosító programot kell bevezetnie, amely magában foglalja a fenyegetések felismerését szolgáló szervezeten belüli és szervezetek közötti információmegosztási képességet.

II.1.16. Kockázatmenedzsment keretrendszer (*)

A Hivatalnak a Kibertv. 6.§ (10) bekezdése alapján nem kell kockázatmenedzsment keretrendszert működtetnie

II.1.17. Kockázatkezelésért felelős szerepkörök (*)

A Hivatalnak a Kibertv. 6.§ (10) bekezdése alapján nem kell kockázatmenedzsment keretrendszert működtetnie.

II.1.18. Ellátási lánc kockázatmenedzsment stratégiája (*)

A Hivatalnak a Kibertv. 6.§ (10) bekezdése alapján nem kell kockázatmenedzsment keretrendszert működtetnie.

II.1.19. Ellátási lánc kockázatmenedzsment stratégia – Üzletmenet (ügymenet) szempontjából kritikus termékek beszállítói (*)

A Hivatalnak a Kibertv. 6.§ (10) bekezdése alapján nem kell kockázatmenedzsment keretrendszert működtetnie.

II.1.20. Folyamatos felügyeleti stratégia (*)

A Hivatalnak ki kell fejlesztenie a folyamatos felügyeleti stratégiát és folyamatos felügyeleti programot működtet, amely magában foglalja:

a) Az egész szervezet számára teljesítménymutatók meghatározását.

b) A felügyelet és a hatékonyság értékelés gyakoriságának meghatározását.

c) A teljesítménymutatók folyamatos, a felügyeleti stratégia szerint történő figyelemmel kísérését.

d) A felügyelet és az elvégzett értékelések adatai közötti összefüggések és információk elemzését. A védelmi intézkedések értékelését és felügyeleti információk eredményéből származtatott válaszlépések megtételét.

e) Az EIR biztonsági állapotáról rendszeres időközönként, a kijelölt személyeknek történő jelentést.

A Hivatal a folyamatos felügyeleti stratégiát a jelen IBSZ *{II.6. 5. Értékelés, engedélyezés és monitorozás}* és a *{II.1.6. A biztonsági teljesítmény mérése}* fejezetében foglalt keretek között valósítja meg.

II.2. SZERVEZETI ARCHITEKTÚRA

A Hivatalnak ki kell fejlesztenie és fenn kell tartania azt a szervezetrendszert, amely tekintettel van mindazon kockázatokra, amelyek hatással lehetnek a Hivatal működésére, az eszközökre, az egyénekre és más szervezetekre.

II.2.1. Az információbiztonsági felelősségi rend meghatározása

Az információbiztonság megteremtése és fenntartása olyan alapvető felelősség, amely szerint nem tartozhat egyszemélyi felelősségi és hatáskörbe az elektronikus információs rendszerek tervezése, fejlesztése, üzemeltetése és felügyelete.

Az információbiztonság megvalósítását, fenntartását és ellenőrzését a Hivatal a feladatok és felelősség szempontjából egymástól elhatárolt szervezeti keretek között, a következők szerint valósítja meg.

II.2.1.1. a Jegyző feladatai

a Jegyző gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:

a) Gondoskodik a szervezet által használt elektronikus információs rendszerek, Hivatali szolgáltatások felméréséről és nyilvántartásba vételéről a következők szerinti bontásban:

aa) a szervezet rendelkezésében lévő elektronikus információs rendszerek;

ab) szervezet által használt központi rendszerek;

ac) a szervezet által igénybe vett, központi szolgáltató által biztosított szolgáltatások és támogató rendszerek;

ad) a szervezet rendelkezésében lévő vagy a szervezet által használt egyéb támogató rendszerek.

b) Meghatározza a Hivatal rendelkezésében lévő, továbbá a szervezet használatában lévő elektronikus információs rendszerek védelmével kapcsolatos szerepköröket, felelősöket, feladatokat és az ehhez szükséges hatásköröket, kinevezi vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt.

c) Gondoskodik a Hivatal rendelkezésében lévő elektronikus információs rendszerekben kezelt adatok felméréséről és osztályozásáról.

d) Az informatikáért felelős miniszter rendelete szerinti hatáselemzést és kockázatmenedzsment tevékenységet végez a Hivatal rendelkezésében lévő elektronikus információs rendszerekre és azok környezetére vonatkozóan.

e) A jogszabályban meghatározottak szerint biztonsági osztályba sorolja a Hivatal rendelkezésében lévő elektronikus információs rendszereket.

f) Meghatározza a Hivatal rendelkezésében lévő elektronikus információs rendszerek vonatkozásában a kockázatokkal arányos védelmi intézkedéseket.

g) Kiadja a felhasználókra és az elektronikus információbiztonsági követelményekre vonatkozó információbiztonsági szabályzatot, valamint gondoskodik annak legalább kétévente vagy a jogszabályban meghatározott esetekben történő felülvizsgálatáról.

h) Biztosítja az elektronikus információs rendszerek védelme vonatkozásában meghatározott védelmi intézkedések teljesülését.

i) Gondoskodik – ha releváns – az európai uniós jogi aktusban foglaltak, valamint az informatikáért felelős miniszter rendelete szerint kiválasztott védelmi intézkedések megfelelőségének első biztonsági osztályba sorolás alkalmával történő értékeléséről.

j) Rendszeresen gondoskodik a védelmi intézkedések időszakos értékeléséről, ennek keretében legalább kockázatelemzések, ellenőrzések, független és a kiberbiztonsági hatóság által kiadott ajánlás szerinti belső kiberbiztonsági értékelés lefolytatása révén meggyőződik arról, hogy a jogszabályoknak és a kockázatoknak megfelelően meghatározott védelmi intézkedések megfelelően biztosítják-e a szervezet és elektronikus információs rendszerei biztonságát.

k) Gondoskodik a biztonsági osztályhoz kapcsolódó védelmi intézkedések értékelése során feltárt hiányosságok orvoslásáról.

l) A szervezeten belül dönt az elektronikus információs rendszerek használatbavételéről vagy használatának folytatásáról.

m) Gondoskodik a kiberbiztonsági hatósági kötelezések teljesítéséről.

n) A j) pontban meghatározott feladatokat a Jegyző legalább kétévente, a biztonsági osztályba sorolás felülvizsgálatával egyidejűleg hajtja végre.

o) Gondoskodik az elektronikus információs rendszerek védelmi feladatainak és az azokhoz kapcsolódó felelősségi köröknek az oktatásáról, saját maga és a szervezet munkatársainak – az informatikáért felelős miniszter rendeletében meghatározott – kiberbiztonsági képzéséről, továbbképzéséről;

p) Biztosítja a kötelezően előírt hazai kiberbiztonsági gyakorlatokon történő részvételt, illetve kiberbiztonsági gyakorlat önálló megtartását;

q) Gondoskodik az elektronikus információs rendszer eseményeinek nyomonkövethetőségéről;

r) Ha szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, illetve a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenység ellátásához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek.

s) Az elektronikus információs rendszert érintő kiberfenyegetés, kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a gyors és hatékony reagálásról, az illetékes kiberbiztonsági incidenskezelő Hivatalnak való bejelentésről, a kiberbiztonsági incidensek kezeléséről, valamint a helyreállításról.

t) Gondoskodik az érintetteknek a kiberbiztonsági incidensekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáról.

u) Gondoskodik a kiberbiztonsági hatóság és az illetékes kiberbiztonsági incidenskezelő Hivatal ajánlásainak, iránymutatásainak az elektronikus információs rendszer védelmének biztosítása érdekében történő figyelembevételéről.

v) Köteles törekedni arra, hogy a jelen jogszabályban meghatározott feladatokat a lehető legrövidebb időn belül hajtsa végre.

w) Gondoskodik arról, hogy a szervezet által az adott évben informatikai fejlesztésre fordított költségek legalább 5%-ának megfelelő összeget a szervezet a tárgyév során kiberbiztonsági fejlesztésekre fordítson.

x) Megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

II.2.1.2. Az IBF

a Jegyző által vállalkozási szerződés keretében megbízott IBF-nek a következők a feladatai, jogai és felelőssége:

II.2.1.2.1. Az IBF feladatai

Az IBF a Hivatal információbiztonsági irányítási rendszerének működtetése és ellenőrzésével kapcsolatos feladatai a következők:

a) Gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.

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

c) Előkészíti és a szervezet vezetőjének jóváhagyását követően megküldi a nemzeti kiberbiztonsági hatóság részére a szervezet információbiztonsági szabályzatát.

d) Előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását.

e) Előkészíti és a szervezet vezetőjének egyetértésével kezdeményezi a nemzeti kiberbiztonsági hatóságnál a szervezet elektronikus információs rendszereivel kapcsolatos engedélyezési eljárásokat.

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

g) Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet elektronikus információbiztonságot érintő szabályzatait és szerződéseit.

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

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

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

k) Legalább évente megvizsgálja a 4. § (2) bekezdése szerinti intézkedési tervet és beszámolót készít a szervezet vezetője számára az előrehaladásról, amiben kiemeli az esetleges lemaradásokat és a rövid távon szükséges intézkedéseket.

l) Kapcsolatot tart a nemzeti kiberbiztonsági hatósággal és a kiberbiztonsági incidenskezelő Hivatallal.

m) A szervezet bármely elektronikus információs rendszerét érintő incidensről tájékoztatja a rendeletben meghatározott szervet.

n) Együttműködik a Kszetv. szerinti kritikus szervezet ellenálló képességéért felelős vezetővel, valamint a Vbö. szerinti ellenálló képességért felelős vezetővel.

II.2.1.2.2. Az IBF jogai

Az IBF a Hivatal információbiztonságának fenntartása érdekében, illetve információbiztonsági incidens esetében jogosult:

a) Külön engedély nélkül a Hivatal bármely helyiségébe belépni, amennyiben ott az információbiztonságot érintő munkavégzés folyik.

b) Bármelyik számítógép, adathordozó vagy számítógépes lista tartalmába betekinteni, függetlenül annak minősítésétől (a vonatkozó jogszabályok betartásával), amennyiben az adott ügyben, illetve témában vizsgálat folyik.

c) Minden értekezleten részt venni, észrevételeit és javaslatait megtenni, amelynek számítástechnikai, illetve információbiztonsági vonatkozása van és ez az értekezlet összehívásakor ismert.

II.2.1.2.3. Az IBF felelőssége

Az IBF felelős a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséért és fenntartásáért.

II.2.1.3. A rendszergazda

A rendszergazda információbiztonsággal kapcsolatos feladata és kötelessége a következő:

II.2.1.3.1. A rendszergazda feladata

A rendszergazda feladatai a következők:

a) Szerverek hardveres és szoftveres karbantartása.

b) Szerverek mentése.

c) Rendszerfelügyelet biztosítása.

d) Rábízott elektronikus információs rendszerek üzemeltetése.

e) A vírusvédelmi rendszer konfigurálása és üzemeltetése.

f) Munkaállomások hardveres és szoftveres karbantartása.

g) A szerverszoba felügyelete.

h) A rendszergazdai teendőkkel összefüggő kimutatások készítése.

i) A felhasználókat érintő rendszerváltozások rögzítése és közzététele.

j) Helyszíni segítségnyújtás a felhasználóknak.

k) Közreműködik a biztonsági incidensek kivizsgálásában.

l) Rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot.

m) Együttműködik az informatikai biztonsággal összefüggő tevékenység végzésében az informatikai biztonságért felelőssel.

n) Amennyiben új fenyegetéseket észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését.

o) Az IBF-fel közösen meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai eszközöket.

p) Kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat.

q) Ellenőrzi a vírusvédelmi programok használatát.

r) Vezeti és naprakészen tartja az IBSZ-ben előírt nyilvántartásokat.

s) Vezeti a Hivatal informatikai eszközeinek és konfigurációjának nyilvántartását.

t) Elvégzi mindazt a feladatokat, melyet az IBSZ a hatáskörébe utal.

II.2.1.3.2. A rendszergazda felelőssége

A rendszergazda felelőssége a Hivatal rendelkezése alatt álló EIR-ek jelen IBSZ-ben foglaltak és az Adminisztrátori dokumentációk szerinti biztonságos üzemeltetése.

II.2.1.4. Az adatgazda

Az adatgazda annak az önálló szervezeti egységnek a vezetője, ahol az adat keletkezik, illetve amelyhez jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését, vagy nyilvántartás vezetését elrendeli.

Az elektronikus információs rendszerek adatgazdáit a Jegyző írásban jelöli ki.

II.2.1.4.1. Az adatgazda feladatai

Az adatgazda információbiztonsággal kapcsolatos feladatai a következők:

a) Az IBF-el közreműködve biztonsági osztályba sorolja a hozzá rendelt elektronikus információs rendszereket.

b) Meghatározza az adatokhoz / tevékenységekhez hozzáférőket, a szükséges-elégséges hozzáférési elv alapján, azaz mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges.

c) Évente - szükség szerint az IBF bevonásával - felülvizsgálja a kiosztott hozzáférési jogokat annak az EIR-nek a vonatkozásában, melynek az adatgazdai feladatait ellátja.

d) Az ügymenet folytonosság tervezése során meghatározza az érintett EIR maximális kiesési idejét és az EIR-ben elfogadható maximális adatvesztés mértékét.

II.2.1.4.2. Az adatgazda felelőssége

Az adatgazda felelős a hatáskörébe tartozó elektronikus információs rendszerek hozzáférési jogosultságainak - a lehetőségek szerint - a „szükséges, minimális jogosultságok” elve alapján történő engedélyezéséért.

II.2.1.5. A szervezeti egység vezetője

A szervezeti egység vezetőjének feladata és felelőssége, hogy az általa irányított szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági előírásokat.

II.2.1.6. A felhasználó

A Hivatal felhasználóinak az elektronikus információs rendszerek biztonságával kapcsolatban a következők a jogai, a kötelességei és a felelőssége:

II.2.1.6.1. A felhasználó jogai

A felhasználó jogosult:

a) A számára biztosított infokommunikációs eszközök, szoftverek üzemszerű használatára.

b) A beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére.

c) Információbiztonsági képzésre.

d) A működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges, általa nem ismert szoftverek használatához támogatást kérni.

e) Meghibásodás, üzemzavar esetén az elhárítás igénylésére.

II.2.1.6.2. A felhasználó kötelessége

Az információk védelmét azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata, életciklusa során biztosítani kell.

Valamennyi felhasználó köteles azonnal értesíteni felettesét a következő eseményekről, körülményekről:

a) az informatikához kapcsolódó tevékenység fennakadása, megszakadása;

b) ha olyan adatokhoz fér hozzá, melynek kezelésében nem illetékes;

c) információbiztonsági esemény.

Az munkahelyi vezetőnek jeleznie kell a tapasztaltakat a rendszergazda részére, aki információbiztonsági incidens esetén értesíti az IBF-et.

Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosítót, jelszót, eToken-t, kulcsot, vagy bárminemű egyéb, a Hivatal erőforrásaihoz hozzáférést biztosító eszközt.

A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással.

Az információbiztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban a felhasználó köteles együttműködni a kivizsgálókkal.

A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, jelszavak kipróbálása, illetve ezek kísérlete is.

II.2.1.6.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a jelen IBSZ *{4. számú melléklet – Felhasználói Informatikai Biztonsági Házirend}* mellékletének megismeréséért és az abban foglalt szabályok betartásáért;

b) a birtokában lévő, vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért;

c) a személyre szóló és védett területre belépést biztosító kártyájának/kártyáinak védelméért és át nem ruházásáért;

d) az elektronikus információs rendszerben végzett műveletekért;

e) a Hivatal elektronikus információs rendszereinek szakszerű kezeléséért és

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

II.2.2. A munkaköri felelősség és az alkalmazás feltételei

A munkaköri leírásokban valamint az álláshelyen ellátandó feladatoknál meg kell határozni az általános és az adott munkakörhöz tartozó információbiztonsági feladatokat és felelősségeket.

A Hivatalnak tájékoztatnia kell a dolgozókat arról, hogy milyen jogi felelősségük és kötelezettségük van az információbiztonsági előírások betartására vonatkozóan. A dolgozók információbiztonsági felelőssége arra az esetre is vonatkozik, ha nem a Hivatalnál (pl. otthon), illetve a normál munkaidőn kívül dolgozik.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák az IBSZ előírásait.

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ *{6. számú melléklet – Felhasználói Nyilatkozat}* mellékletében található nyilatkozat aláírása után lehet használatba venni.

II.3. HOZZÁFÉRÉS-FELÜGYELET

A technológiai vhr **HOZZÁFÉRÉS-FELÜGYELET** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.3.1. Szabályzat és eljárásrendek

A hozzáférés-felügyeleti eljárásrendet az IBSZ jelen fejezete tartalmazza.

II.3.2. Fiókkezelés

Elektronikus információs rendszerenként meg kell határozni, hogy milyen típusú fiókok engedélyezettek (pl.: általános, megosztott, csoport, gyártói/fejlesztői/szállítói, ideiglenes, vendég, technikai).

Meg kell határozni azokat az alapfunkciókat (alapjogosultságokat), melyeket munkakörökhöz lehet rendelni és ezeket a jogosultságokat a felhasználók automatikusan megkaphatják a munkakör betöltésekor.

Elektronikus információs rendszerenként dokumentálni kell az érintett EIR-ben létrehozott szerepköröket és a szerepkörökhöz rendelt jogosultságokat (szerepkör-jogosultsági mátrix).

A Hivatal EIR-jeihez hozzáférési jogosultságokat a Hivatal Szervezeti és Működési Szabályzata alapján meghatározott alapfunkciók alapján, vagy egyedi igénylések alapján lehet biztosítani.

A beépített adminisztrátori és vendég fiókokat valamennyi eszközön tiltani kell.

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.

A jogosultságok és a hozzáférés menedzselésekor az alábbi alapelveket kell figyelembe venni:

a) A meghatározott jogosultságok alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés kockázata.

b) Az elektronikus információs rendszerrel kapcsolatba kerülő személyeknek a munkájuk ellátásához szükséges minimális jogosultságokat kell biztosítani a munkavégzésük időtartamára.

c) Az azonos tevékenységet ellátó felhasználók jogosultságai szerepkörök szintjén legyenek kialakítva, és a felhasználók a kialakított szerepkörökbe kerüljenek besorolásra.

d) Az összeférhetetlenségi szabályokat figyelembe kell venni.

e) Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságokat adminisztrálni kell.

f) Törekedni kell arra, hogy a jogosultságok automatizált módon kerüljenek nyilvántartásba, szükség esetén papír alapon kell a nyilvántartást vezetni.

g) Minden egyes elektronikus információs rendszerhez csak a megfelelő adminisztrálást követően lehet felhasználói jogosultságot adni, módosítani, és felfüggeszteni, illetve visszavonni.

h) Az éles elektronikus információs rendszerekben a fejlesztők hozzáférési jogosultságokkal nem rendelkezhetnek.

A felhasználók nyilvántartásba vételi szabályainak és a követendő eljárásrend kidolgozásakor a következőket kell figyelembe venni:

a) A felhasználói tevékenység ellenőrizhetősége és nyomon követhetősége érdekében a felhasználók elektronikus információs rendszerekben történő azonosítására egyedi felhasználó azonosítókat kell alkalmazni.

b) A csoportos felhasználó azonosítók használatát tiltani kell.

c) A felhasználói hozzáférési jogosultságokat a szervezeti egység vezetője határozza meg. A jogosultság meghatározása során figyelembe kell venni:

    i. a felhasználó munkakörét és az azzal kapcsolatos feladatait;

    ii. a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultságok elvét;

    iii. a felhasználó jogviszonyát;

    iv. a felhasználó munkahelyét.

d) A jogosultság igénylését tartalmazó dokumentumnak tartalmaznia kell:

   i. a felhasználó nevét, munkakörét, szervezeti egységét és munkahelyét;

   ii. annak megjelölését, hogy milyen szolgáltatásokhoz történik a jogosultságigénylés;

   iii. azt, hogy az érintett szolgáltatások tekintetében milyen szerepkör, vagy hozzáférési jogok (olvasás, bevitel/bővítés, törlés, módosítás, teljes) igénylése történik;

   iv. annak megjelölését, hogy az érintett szolgáltatások és jogosultságok igénylése milyen adatkörre vonatkozóan történik;

   v. a munkahelyi vezető aláírását.

A jogosultságigénylési lapot az igényelt és a beállított jogosultságok egyeztetése céljából a rendszergazda tárolja.

A jogosultságok kezelését dokumentált formában kell kezelni. Minden kiosztott jogosultságról nyilvántartást kell vezetni.

A nyilvántartásban a következőket kell rögzíteni:

a) Felhasználó neve;

b) Felhasználó beosztása;

c) Felhasználó szervezeti egysége;

d) Érintett EIR;

e) Szerepkör(ök), jogosultságok megnevezése;

f) Kiadás dátuma;

g) Visszavonás dátuma;

h) Beállító, visszavonó rendszergazda neve.

II.3.3. Kiemelt jogosultságok kezelése

A felhasználói jogosultságok kiadási folyamatánál szigorúbban kell kezelni a kiemelt jogokat biztosító adminisztrátori jogok megadását.

Az elektronikus információs rendszereknél a jogosultságok kiadásának engedélyezési eljárása során az alábbiakat kell figyelembe venni:

i) Pontosan meg kell határozni azokat a rendszerelemeket, - pl. operációs rendszereket, adatbázis kezelő rendszert, valamint az alkalmazásokat - és az alkalmazotti kategóriát, amelyhez az adminisztrátori jogosultságokat kell hozzá rendelni.

j) Az adminisztrátori jogosultságokat a „feltétlenül szükséges” és az „eseményenkénti” használat elve alapján kell kiadni.

k) Az adminisztrátori jogot kizárólag a Jegyző engedélyezheti írásban.

l) Technikai azonosító részére adminisztrátori jogot az IBF engedélyezi írásban.

Az üzemeltetők csak az elektronikus információs rendszer, illetve alkalmazás üzemeltetéséhez szükséges információkhoz férhetnek hozzá, a részükre biztosított adminisztrátori jogosultság birtokában csak a felhasználó külön engedélyével és jelenlétében, kifejezetten a hiba elhárítása érdekében, vagy a felhasználói igény kielégítése érdekében férhetnek hozzá a felhasználók által kezelt információkhoz.

A rendszergazda nem küldhet levelet más felhasználó nevében.

II.3.4. Hozzáférési jogok igénylésének eljárásrendje

Az új hozzáférési jogok igénylését, a jogosultságok módosítását és a jogosultságok visszavonását a jelen fejezetben leírtak szerint kell elvégezni.

II.3.4.1. Új hozzáférési jog igénylése

Az igénylő a hozzáférési jogok igénylését a jelen IBSZ *{3. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található űrlap kitöltésével kezdeményezi. Hozzáférési jogot az igényelhet, akinek a feladatellátásához az szükséges.

Az űrlapon meg kell jelölni az igényelt jogosultság szintjét, azt az időszakot, amelyre a jogosultságot biztosítani kell, illetve a jogosultságigénylés indoklását.

A kitöltött űrlapot alá kell írattatni a munkahelyi vezetővel, aki igazolja, hogy a feladatellátáshoz szükséges a jogosultság biztosítása.

Az űrlapot ezután meg kell küldeni az adatgazda részére, aki jóváhagyja a jogosultságigénylést.

A jóváhagyott jogosultságigénylési űrlapot ezután el kell küldeni a rendszergazda részére, aki intézkedik a jogosultság kiadásáról.

A feldolgozás első lépése: A rendszergazda rögzíti az igényt a jogosultság-nyilvántartásban.

A feldolgozás második lépése: A rendszergazda az igényelt beállításokkal létrehozott felhasználói fiókról telefonon vagy személyesen értesíti az igénylőt, megadja a belépéshez használatos felhasználói nevet, az első belépést lehetővé tevő kezdeti jelszót és szükség esetén egyéb fontos adatokat. Telefonos kapcsolat esetén az igénylőlapon rögzített információk alapján azonosítani kell az igénylőt.

A feldolgozás harmadik lépése: A kért feladatok elvégzésének bizonylatolása érdekében a rendszergazda aláírja a kitöltött jelen IBSZ *{3. számú melléklet – Jogosultságigénylési űrlap}* mellékletét, valamint e-mailen tájékoztatja az igénylőt és a jóváhagyót a jogosultságok megadásáról és a felhasználói névről.

Az aláírt űrlapokat a rendszergazda tárolja visszakereshető formában.

Az IBF az említett adatlapok meglétét és a tényleges jogosultság kiadását bármikor ellenőrizheti, és véleményét írásba foglalhatja, amelyet a Hivatal a jogosultsági rendjének folyamatos javítására használ fel.

II.3.4.2. Hozzáférési jog módosítása

A munkahelyi vezető a dolgozó megváltozott feladatkörének, illetve munkakörének ellátásához szükséges jogosultság módosításához kitölti a jelen IBSZ *{3. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található űrlapot.

Az eljárásrend megegyezik a *{II.3.4.1 Új hozzáférési jog igénylése}* fejezetben leírtakkal annyi kiegészítéssel, hogy amennyiben szervezeti egység váltás történik, akkor a rendszergazda gondoskodik a már nem szükséges jogosultságok visszavonásáról.

II.3.4.3. Hozzáférési jog visszavonása

A munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. A hozzáférési jogosultság visszavonását a jelen IBSZ *{3. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található űrlapon kell kezdeményezni.

Az űrlapot ezután el kell küldeni a rendszergazda részére, aki intézkedik a jogosultság visszavonásáról.

A feldolgozás első lépése: A rendszergazda rögzíti az igényt a jogosultság nyilvántartásban.

A feldolgozás második lépése: A rendszergazda visszavonja a jogosultságot.

A feldolgozás harmadik lépése: A rendszergazda aláírja a jelen IBSZ *{3. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található, kitöltött űrlapot, valamint e-mail-en tájékoztatja a munkahelyi vezetőt a visszavonás tényéről.

II.3.5. Jogosultságok nyilvántartása

Jogosultságnyilvántartást kell vezetni az EIR-ekben kiosztott jogosultságokról. A nyilvántartásnak a következő adatokat kell tartalmaznia:

A nyilvántartás vezetése és naprakészen tartása a rendszergazda feladata és felelőssége.

a) EIR neve;
b) EIR leírása;
c) EIR adatgazdája;
d) EIR üzemeltetője, rendszergazdája;
e) felhasználó neve;
f) felhasználó szervezeti egysége;
g) felhasználó beosztása;
h) felhasználó azonosítója;
i) jogosultság érvényessége (aktív, letiltott)
j) jogosultság kezdete;
k) jogosultság vége;
l) hozzáférési szint:
    a. privilegizált;
    b. nem-privilegizált.
m) szerepkör megnevezése;
n) jogosultságot beállító neve.
o) utolsó felülvizsgálat ideje;
p) utolsó felülvizsgálatot elvégző neve.

A szerepkörök konkrét jogosultságainak a leírását szerepkör-jogosultság mátrix-ban kell definiálni.

A mátrix-ot az érintett EIR szállítójának kell elkészítenie és rögzítenie az EIR rendszerdokumentációjában.

II.3.6. Regisztráció külső honlapokra

Külső honlapokra történő regisztrációt az adatgazdánál kell kezdeményezni az érintett munkatárs vezetőjének előzetes jóváhagyásával.

A jogosultságokról az érintett adatgazda nyilvántartást vezet a következő tartalommal:

a) honlap neve;

b) honlap leírása;

c) honlap adatgazdája;

d) honlap üzemeltetője;

e) felhasználó neve;

f) felhasználó szervezeti egysége;

g) felhasználó beosztása;

h) felhasználó azonosítója;

i) jogosultság kezdete;

j) jogosultság vége;

k) jogosultság leírása.

Változás esetén (felhasználói jogosultság visszavonása, módosítása) az érintett vezetőnek tájékoztatást kell adnia a rendszergazda részére, aki átvezeti azt a nyilvántartásban.

A külső honlapok jogosultságait - az érintett honlap adatgazdájának bevonásával – évente a rendes jogosultság felülvizsgálattal párhuzamosan felül kell vizsgálni és a szükséges módosításokat át kell vezetni a nyilvántartásba, illetve kezdeményezni kell azt az érintett honlap üzemeltetőjénél.

II.3.6.1. A felhasználói hozzáférési jogok felülvizsgálata

Ellenőrizni kell, hogy a kiadott hozzáférési jogosultságok szintje alkalmas-e a kívánt célra (biztosítja-e az elvárt logikai védelmet). Ennek érdekében az EIR-ek kiosztott hozzáférési jogosultságait az érintett EIR adatgazdája – szükség szerint az IBF bevonásával - évente felülvizsgálja.

II.3.7. Hozzáférés ellenőrzés érvényre juttatása

Az elektronikus információs rendszereknek az IBSZ-szel összhangban érvényre kell juttatnia a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

II.3.8. Sikertelen bejelentkezési kísérletek (*)

Az EIR-ekbe történő bejelentkezések során 5 sikertelen bejelentkezési kísérlet után 30 percre zárolni kell az érintett fiókot. A számlálót 30 perc után lehet nullázni vagy a fiókot csak a rendszergazda engedélyezheti újra.

II.3.9. A rendszerhasználat jelzése (*)

Az EIR-ekbe történő bejelentkezés előtt ki kell jelezni a felhasználó számára, hogy a felhasználó a Hivatal adott éles rendszerét használja és a bejelentkezéssel egyidejűleg a beleegyezését adja:

a) A Hivatal a rendszer használatát figyelheti, rögzítheti, naplózhatja.

b) A rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár.

Az EIR-nek mindaddig fenn kell tartania a rendszerhasználati értesítést a képernyőn, amíg a felhasználók nem fogadják el a használati feltételeket és nem tesznek egyértelmű lépéseket a rendszerbe való bejelentkezésre, vagy a rendszerhez való további hozzáférésre.

Nyilvánosan hozzáférhető rendszerek esetén az értesítés legalább az alábbiakat tartalmazza:

a) A felhasználók a szervezet EIR-ét használják.

b) A rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják.

c) A rendszer jogosulatlan használata tilos és büntető-, vagy polgári jogi felelősséggel jár.

II.3.10. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

A Hivatal EIR-jeiben – az azonosítási és hitelesítési felület elérésén kívül – nem engedélyezettek a hitelesítés nélkül engedélyezett tevékenységek.

II.3.11. Felelősségek szétválasztása (*)

A Hivatalban információbiztonsági szempontból a következő összeférhetetlenségi szabályokat kell alkalmazni:

a) a Jegyző, a gazdasági vezetői feladatait ellátó személy, és a felhasználó továbbá, aki a Hivatalon belül informatikai üzemeltetéssel, informatikai fejlesztéssel kapcsolatos munkakört lát el, nem láthatja el az IBF feladatait.

b) Az IBF-nek függetlennek kell lennie, kizárólag a Jegyzőnek tartozik beszámolási kötelezettséggel és nem láthat el semmilyen informatikai feladatot.

c) A rendszergazda és a támogató a főszabály szerint nem végezhet fejlesztési tevékenységeket. Amennyiben erre szükség van, akkor azt szabályozni kell a vállalkozási szerződésben és megfelelően külön határolt módon kell a két tevékenységet végezni.

d) A fejlesztő nem végezhet üzemeltetési tevékenységet. Amennyiben erre szükség van, akkor azt szabályozni kell a vállalkozási szerződésben és megfelelően külön határolt módon kell a két tevékenységet végezni.

A fenti elveket az EIR-ek jogosultságkezelésében is érvényesíteni kell.

II.3.12. Távoli hozzáférés (*)

A Hivatal belső elektronikus információs rendszereinek külső hozzáférése során ismert sérülékenységektől mentes, mértékadó szervezet, illetve dokumentum által biztonságosnak minősített kriptográfiai algoritmus által titkosított VPN kapcsolatot kell alkalmazni, melynek során egyedileg kell azonosítani a felhasználót.

A következő VPN protokollok engedélyezettek:

a) Open VPN;

b) IPsec VPN;

c) SSL VPN.

A távoli hozzáférek során többtényezős azonosítást és hitelesítést kell alkalmazni.

A VPN kapcsolat során naplózni kell a sikeres és a sikertelen hozzáférési kísérleteket. Nagyszámú sikertelen hozzáférési kísérlet esetén riasztást kell küldeni a rendszergazdák részére.

Szokatlan eseményekre utaló jeleket keresve rendszeresen át kell vizsgálni a VPN naplókat.

A munka befejeztével bontani kell a VPN kapcsolatot.

A VPN kapcsolatot végződtető eszközt külön hálózati szegmensbe (továbbiakban: VPN szegmens) kell telepíteni és a belső hálózat, valamint a VPN szegmens közötti forgalmat a Hivatali tűzfalon keresztül kell felügyelni. A két szegmens között csak és kizárólag a működéshez szükséges forgalom engedhető át.

A Hivatal belső elektronikus információs rendszereinek külső hozzáféréséhez csak olyan biztonságos infokommunikációs eszköz használható, amely megfelel a következő követelményeknek:

a) Az eszközökön a felhasználóknak rendszergazdai jog nem adható.

b) Az eszközökön naprakész kártékony kód elleni védelmet kell megvalósítani.

c) Az eszközökön az operációs rendszer és a felhasználói programok naprakészségét biztosítani kell.

d) Az eszközökön bekapcsolt tűzfalat kell alkalmazni.

Magán felhasználásban lévő eszköz esetében törekedni kell arra, hogy csak a képernyőkép kerüljön átvitelre a felhasználó számára.

A felhasználók képzésénél kiemelt figyelmet kell fordítani ezen eszközök biztonságos kezelésére.

Privilegizált hozzáférési jogosultsággal történő VPN kapcsolat létrehozásánál a következők szerint kell eljárni:

a) IP szinten korlátozni szükséges a kapcsolódást;

b) többtényezős azonosítás és hitelesítést kell alkalmazni;

c) naplózni és monitorozni kell a sikeres és sikertelen hozzáférési kísérleteket;

d) csak menedzselt hozzáférési ponton keresztül lehet a hozzáférést biztosítani és csak ahhoz az eszközhöz, amelyhez a feladat elvégzéséhez szükség van;

e) törekedni kell arra, hogy a VPN kapcsolat során csak a képernyő kerüljön átvitelre.

II.3.13. Vezeték nélküli hozzáférés (*)

A Hivatalban csak az IBF által jóváhagyott 802.11x alapú vezeték nélküli (továbbiakban: Wi-Fi) hozzáférési pont létesíthető.

A Hivatalban ad-hoc Wi-Fi hálózat, mikrohullámú, nagyon magas- vagy ultra magas frekvenciájú rádió frekvencia és a Bluetooth kapcsolat nem létesíthető.

Valamennyi hozzáférési pontot a Hivatal által biztosított eszközön kell létrehozni. Idegen Wi-Fi router-t tilos a Hivatal hálózatába csatlakoztatni.

Minden hozzáférési pont részére külön VLAN-t kell létrehozni, úgy hogy a hálózatok között nem lehet átjárás és az egy hálózatban lévő eszközök sem érhetik el egymást. Biztosítani kell a hozzáférési pontok felügyeletét.

Az internet és a belső hálózat elérése a Hivatali tűzfalon keresztül történhet.

A Hivatal hálózatában csak olyan Wi-Fi hozzáférési pont létesíthető, amely minimum WPA2 hitelesítést és titkosítást alkalmaz.

A Hivatal belső hálózatából a munkaállomásokról és laptopokról tilos mobil internet megosztással internetelérést kezdeményezni.

II.3.13.1. Vezeték nélküli hozzáférés – Hitelesítés és titkosítás

Valamennyi hozzáférési pont esetében ismert sérülékenységektől mentes, mértékadó szervezet, illetve dokumentum által biztonságosnak minősített kriptográfiai algoritmus megvalósított azonosítást és hitelesítést kell alkalmazni.

Kockázat elemzéssel kell meghatározni a szükséges védelmet és a megfelelő hitelesítési módszert.

A kiosztott kulcsok létrehozására vonatkozóan a következőket kell követni:

a) A kulcs hossza minimum 12 karakter.

b) A kulcs tartalmazzon kisbetűt, nagybetűt, számot vagy speciális karaktert.

A kulcsot 6 havonta meg kell változtatni.

II.3.14. Mobil eszközök hozzáférés-ellenőrzése (*)

Mobil eszközzel csak a Hivatal által biztosított elektronikus levelezéshez lehet hozzáférni. A Hivatal által biztosított elektronikus levelezéshez csak olyan eszközzel lehet hozzáférni, melyen

a) gyártó által támogatott, naprakész operációs rendszer fut,

b) kártékony kód elleni védelem telepítésre került

c) valamilyen hozzáférés elleni védelem (jelszó, pin kód, biometrikus azonosítás stb.) bekapcsolásra került;

d) az eszköz szabványos, sérülékenységektől mentes kriptográfiai algoritmussal titkosításra került.

II.3.15. Mobil eszközök hozzáférés-ellenőrzése – Teljes eszköz vagy konténer-alapú titkosítás (*)

A következő mobil eszközökön teljes eszköz vagy konténer alapú titkosítást kell alkalmazni:

a) okostelefon;

b) memória kártya;

c) tablet;

d) notebook;

e) mobil merevlemez;

f) pen-drive.

Titkosítást ismert sérülékenységektől mentes, mértékadó szervezet, illetve dokumentum által biztonságosnak minősített kriptográfiai algoritmussal kell megvalósítani. A titkosítás során alkalmazott kulcsméretet a vonatkozó ajánlások alapján kell kiválasztani.

II.3.16. Külső elektronikus információs rendszerek használata

A Hivatal elektronikus információs rendszereiben kezelt adatok külső fél részére történő továbbítása előtt az érintett felhasználónak meg kell vizsgálnia, hogy a vonatkozó szerződés vagy jogszabály alapján az adat átadható-e. Különös figyelmet kell fordítani a jogszabály által védett adatok továbbítására.

Az információ megosztással kapcsolatos követelményeket az adott terület vezetőjének ismertetnie kell a felhasználókkal.

II.3.17. Nyilvánosan elérhető tartalom

Az információk közzétételével kapcsolatban a Hivatal a jogszabályokat, a vonatkozó belső szabályzatát és az erkölcsi normákat követi.

A nyilvános tartalmak kezelésével kapcsolatban a következők szerint kell eljárni:

a) Ki kell jelölni azokat a személyeket, akik jogosultak a Hivatal honlapján a Hivatal és a Hivatal működésével kapcsolatos bármely információ közzétételére.

b) A kijelölt személyeket képzésben kell részesíteni annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános (pl.: személyes adatokat, üzleti titkokat) információkat.

c) Gondoskodni kell arról, hogy közzététel előtt átvizsgálásra kerüljenek a publikálandó tartalmak

d) Időszakosan át kell vizsgálni a Hivatal honlapját a nem nyilvános információk tekintetében, és gondoskodni kell azok eltávolításáról.

II.4. TUDATOSSÁG ÉS KÉPZÉS

A technológiai vhr **TUDATOSSÁG ÉS KÉPZÉS** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza

II.4.1. Szabályzat és eljárásrendek

A tudatossági és képzési eljárásrendet az IBSZ jelen fejezete tartalmazza.

II.4.2. Biztonságtudatossági képzés

Rendszeres belső oktatásokkal gondoskodni kell arról, hogy a felhasználókban tudatosodjanak az alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő információbiztonsági fenyegetettségeket. Gondoskodni kell arról is, hogy a napi feladatok végzése során a felhasználók kellőképpen felkészültek legyenek a jelen IBSZ-ben foglaltak betartására.

II.4.2.1. Alap biztonság tudatossági képzés

Minden felhasználó részére alap biztonság tudatossági képzéseket kell tartani. A képzésen a következő témaköröket kell érinteni:

a) információbiztonságra vonatkozó jogszabályok;
b) információbiztonsági alapfogalmak;

c) alapvető biztonsági követelmények;
d) felhasználók napi munkavégzése során jelentkező fenyegetettségek;
e) a lehetséges fenyegetések felismerése;
f) fenyegetettségekkel szembeni védekezési lehetőségek;
g) Hivatal információbiztonsági szabályozó rendszerének ismertetése.

Új dolgozó munkába lépésekor a dolgozóval a munkába állás előtt az információbiztonsági előírásokat meg kell ismertetni. A dolgozók információbiztonsági tudatosságának fenntartása érdekében évente frissítő oktatást kell szervezni.

Az információbiztonsági oktatások és továbbképzések tematikájának kidolgozása, a szükséges szakirodalom és tájékoztató anyagok biztosítása, valamint a képzés megtartása az IBF feladata.

Az oktatáson, illetve továbbképzésen való részvétel az elektronikus információs rendszerrel kapcsolatba kerülő személyek számára kötelező és a megjelenést a résztvevők aláírásukkal kötelesek tanúsítani.

II.4.2.2. Frissítő biztonság tudatosági képzés

Éves gyakorisággal frissítő biztonság tudatossági képzést kell tartani valamennyi felhasználó részére. A képzésen történő részvétel kötelező.

A képzés tematikáját az IBF-nek kell összeállítani. A képzést az IBF tartja meg.

II.4.3. Biztonságtudatossági képzés – Belső fenyegetés (*)

A biztonság tudatossági képzéseken ki kell térni a belső fenyegetések ismertetésére és az azok elleni védekezésre.

II.4.4. Szerepkör alapú biztonsági képzés (*)

a Jegyzőnek, a rendszergazdának és az IBF-nek a következő, külön jogszabályban előírt továbbképzésen és éves továbbképzésen kell részt venniük:

Szerepkör megnevezése	Képzés megnevezése
Jegyző	Elektronikus információs rendszerek védelméért felelős vezető (Nemzeti Közszolgálati Egyetem)
Rendszergazda	Elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy (Nemzeti Közszolgálati Egyetem)
IBF	NKE végzettség esetén elektronikus információbiztonsági vezető
	A képzési rendelet 7. § (2) bekezdése szerinti nemzetközi minősítések esetében az adott minősítés fenntartásának biztosítása

II.4.5. A biztonsági képzésre vonatkozó dokumentációk

A Hivatal a biztonságtudatosságra vonatkozó alap, frissítő, szerepkör vagy feladat alapú biztonsági képzések oktatási anyagait visszakereshető formában dokumentálnia kell, a képzésen résztvevők a jelenléti ív aláírásával elismerik a képzés, oktatás megtörténtét és az információbiztonsági előírások megismerését.

Nyilvántartást kell vezetni a biztonság tudatossági képzésekről. A nyilvántartásban a következő adatokat kell szerepeltetni:

a) Képzés megnevezése;

aa) alap-, szerepkör vagy feladat;

b) Képzés dátuma;

c) Időtartama;

d) Képzésen részt vevők létszáma;

e) Jelenléti ív iktatószáma;

f) Oktatási anyag elérhetősége;

A képzést dokumentálni kell az oktatási anyagok (előadás diák, tesztek) és jelenléti ívek formájában. Az oktatási anyagokat visszakereshető formában tárolni szükséges a hatósági ellenőrzéseken történő bemutatás érdekében.

II.5. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

A technológiai vhr **NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG** kontrollcsalád JELENTŐS biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.5.1. Szabályzat és eljárásrendek

A naplózásra és elszámoltathatóságra vonatkozó szabályzatot és a naplózási és elszámoltathatósági eljárásrendet az IBSZ jelen fejezete tartalmazza.

II.5.2. Naplózható események

Az EIR-ek naplózásának kialakításakor biztosítani kell, hogy a naplóbejegyzésekből az alábbi információk megállapíthatóak legyenek:

a) milyen típusú esemény történt;

b) mikor történt az esemény;

c) hol történt az esemény;

d) miből származott az esemény; és

e) mi volt az eseménynek a kimenetele, valamint

f) az eseményhez kapcsolódó személyek, alanyok, objektumok.

Az elektronikus információs rendszerek naplózható és egyben naplózandó eseményei a következők:

a) a felhasználók adminisztrációs tevékenysége:

ab) bejelentkezés;

ac) kijelentkezés;

ad) jelszómódosítás.

b) az adatállományok (adatbázisok) módosítása az alkalmazási rendszerekben;

c) a privilegizált felhasználók (alkalmazás adminisztrátorok, rendszergazdák) a rendszer bármely rétegébe történő be-és kijelentkezése;

d) a privilegizált felhasználók (alkalmazás adminisztrátorok, rendszergazdák) tevékenysége a rendszer bármely rétegében;

e) a felhasználói jogosultságok módosítása;

f) rendszer események, esetleges hibák;

g) konfigurációs beállítások módosítása.

h) Az esemény típusának megfelelően az általános feldolgozási eseményt az eseménynaplóban, a biztonsággal összefüggő eseményeket pedig a biztonsági naplóba kell rögzíteni.

Az elektronikus információs rendszerek naplózása kialakításakor be kell vonni a rendszer adatgazdáját is, annak érdekében, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletinformációk, amelyeket az adatgazdák igényelnek.

II.5.3. Naplózandó események

A Hivatal EIR-jeinek a jelen IBSZ *{II.5.2. Naplózható események}* fejezetében foglalt eseményeket kell naplóznia.

II.5.4. Naplóbejegyzések tartalma

A naplóbejegyzéseknek a következőket kell tartalmaznia:

a) a rendszerelem azonosítóját;

b) az adatazonosítót (fájl / rekord / mező);

c) az esemény ismertetését / a funkcióazonosítót;

d) a felhasználó azonosítóját;

e) az esemény időpontját;

f) az esemény elemzéséhez szükséges adattartalmakat vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát.

II.5.5. Naplózás tárkapacitása

A naplók tárkapacitását az adott rendszer fejlesztőjének a bevonásával vagy ajánlásai alapján az előzetes kapacitástervezési folyamat során kell kialakítani figyelemmel a jelen IBSZ *{II.5.2. Naplózható események}* pontjában előírt követelményekre.

A napló tárkapacitás figyelését a rendszerek felügyeleti tevékenységébe kell beépíteni.

A naplózást úgy kell beállítani, hogy amennyiben a napló betelik, úgy automatikusan kerüljön archiválásra a napló, ezzel biztosítva a naplóbejegyzések felülírásának megakadályozását, vagy

küldjön automatikus értesítést a rendszer a rendszergazdának és további (naplózandó) tevékenység elvégzését ne engedje a tárkapacitás növeléséig.

II.5.6. Naplózási hiba kezelése

A Hivatal elektronikus információs rendszereiben a naplók figyelését oly módon kell kialakítani, hogy naplózási hiba esetén küldjön riasztást a rendszert üzemeltető rendszergazdáknak és a naplózási hiba kijavításáig újabb tevékenység ne legyen végrehajtható az EIR-ben.

II.5.7. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

A Hivatal EIR-jeiben az eseménynaplókat és biztonsági naplókat a heti és havi üzemeltetési feladatok során át kell vizsgálni.

A hibabejegyzéseket és a szokatlan működésre utaló jeleket a *{II.19.2. Hibajavítás}* fejezetben leírtak alapján kell kezelni.

A biztonsági eseményre utaló jeleket a jelen IBSZ *{II.10. Biztonsági események kezelése}* fejezet szerint kell kezelni.

Biztonsági eseményre utaló jelek esetén, amennyiben a jelenlegi naplózás nem mutat eredményt, meg kell emelni a naplózás szintjét.

II.5.8. Időbélyegek

Az elektronikus információs rendszereknek a naplóbejegyzésekhez készített időbélyegeket a rendszer belső órái alapján kell elkészítenie.

A Hivatalnak szinkronizálnia kell az EIR-ek belső rendszer óráit a belső hálózatban kijelölt eszközhöz, a kijelölt eszköznek pedig külső, megbízható időszolgáltatóhoz kell szinkronizálnia.

II.5.9. Naplóinformációk védelme

Az elektronikus információs rendszereknek a jelen IBSZ-ben foglaltaknak megfelelően meg kell védenie a napló információkat és a napló eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

II.5.10. A naplóbejegyzések megőrzése

A biztonsági események utólagos kivizsgálása érdekében a naplóbejegyzéseket 1 évig meg kell őrizni.

II.5.11. Naplóbejegyzések létrehozása

Olyan elektronikus információs rendszereket kell alkalmazni, melyek

q) biztosítják a naplóbejegyzések előállítási lehetőségét a jelen IBSZ *{II.5.2. Naplózható események}* pontban meghatározott naplózható eseményekre;

r) lehetővé teszik meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire;

s) naplóbejegyzéseket állít elő a jelen IBSZ *{{II.5.2. Naplózható események}* pontban meghatározottak szerinti eseményekre az jelen IBSZ *{II.5.4. Naplóbejegyzések tartalma}* pontban meghatározott tartalommal.

II.6. 5. ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS

A technológiai vhr **ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.6.1. Szabályzat és eljárásrendek

A Hivatal biztonságértékelési szabályzatát az IBSZ jelen fejezete tartalmazza.

II.6.2. Biztonsági értékelések (*)

A Kibertv. 6.§ (10) bekezdése alapján a Hivatalnak nem kell biztonsági értékeléseket végeznie.

II.6.3. Információcsere (*)

A Hivatalnak jóvá kell hagynia és szabályoznia kell az információcserét az EIR és más rendszerek között, összhangban a kapcsolódásokra és az információcserére vonatkozó biztonsági megállapodásokkal, továbbá figyelembe veszi a szolgáltatási szintre, a felhasználókra és a titoktartásra vonatkozó, valamint a szervezet által meghatározott egyéb megállapodásokat.

Minden egyes információcsere-megállapodás keretében dokumentálja az egyes rendszerek interfészeinek jellemzőit, biztonsági követelményeit, védelmi intézkedéseit és felelősségi körét, valamint rögzíti a megosztott információk hatásának szintjét is.

A Hivatal EIR-jeinek felügyelet nélküli összekapcsolása más szervezetek informatikai rendszerével nem engedélyezett.

Az összekapcsolást mind a Jegyzőnek, mind a rendszergazdának, mind pedig az IBF-nek is jóvá kell hagynia.

Az engedélynek tartalmaznia kell az összeköttetés pontos paramétereit, interfész-leírását (cél, technikai megvalósítás, átvitt információk, biztonsági követelmények).

Dokumentálni kell az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

Más kapcsolódó szervezet csak a Hivatal által nyújtott interfészen keresztül csatlakozhat a Hivatal EIR-jeihez.

Szerződésben vállalnia kell a kapcsolódó szervnek, hogy biztosítja a saját elektronikus információs rendszerében a cél elektronikus információs rendszer biztonsági osztályának megfelelő, a technológiai vhr által előírt követelmények teljesülését.

Információbiztonsági incidens esetén a Hivatal jogosult a kapcsolatot felfüggeszteni.

Az átvitt adatok bizalmasságának és sértetlenségének biztosításáról ismert sérülékenységektől mentes, mértékadó szervezet, illetve dokumentum által biztonságosnak minősített kriptográfiai algoritmus alkalmazásával kell gondoskodni.

Technikai úton korlátozni kell a kapcsolódást.

Rendszeres időközönként felülvizsgálja és frissíti a megállapodásokat.

A változások lekövetésére a megállapodásokat 2 éves gyakorisággal felül kell vizsgálni. Soron kívül felül kell vizsgálni a megállapodásokat, ha a Hivatal szervezetében vagy az EIR-jeiben jelentős változás áll be.

A rendes és a soron kívüli felülvizsgálatot az informatikai területért felelős vezető végzi el.

II.6.4. Az intézkedési terv és mérföldkövei

Az IBF-nek a jelen IBSZ kiadását követően 90 napon belül intézkedési tervet kell készítenie a biztonsági szinthez tartozó követelmények, előírások teljesítésére, illetve javítására, valamint a következő biztonsági osztály elérésére vonatkozóan.

Az intézkedési tervet a Jegyző hagyja jóvá. Az intézkedési tervet az IBF-nek évente felül kell vizsgálnia.

II.6.5. Engedélyezés (*)

A Hivatalnak ki kell jelölnie

a) egy engedélyezésért felelős személyt, aki az EIR-ért felel.

b) egy felelős személyt, aki a szervezeti EIR-ekre vonatkozó közös, más rendszerekből áthozott (átörökített) biztonsági követelmények elfogadásáért felel.

Az engedélyezésért felelős személy az EIR használatbavételét megelőzően:

a) elfogadja a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények alkalmazását; és

b) a szervezet vezetőjével engedélyezteti a rendszer működését.

c) Biztosítja, hogy a közös biztonsági követelményekért felelős személy engedélyezze a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények használatát.

d) Rendszeresen felülvizsgálja az engedélyeket.

Az engedélyezési felelős személy feladatait az EIR adatgazdája látja el.

II.6.6. Folyamatos felügyelet (*)

A Hivatalnak ki kell dolgoznia a rendszerszintű folyamatos felügyeleti stratégiát és megvalósítja a folyamatos felügyeletet a szervezeti szintű stratégiával összhangban, amely magában foglalja a következőket:

a) A rendszerszintű metrikák meghatározását.

b) Rendszeres felügyelet biztosítását a védelmi intézkedések hatékonyságának értékelésére.

c) A védelmi intézkedések folyamatos értékelését.

d) Az EIR és a szervezet által meghatározott mutatók folyamatos nyomon követését.

e) A védelmi intézkedésekről gyűjtött és feldolgozott információ összegzését és kiértékelését.

f) A védelmi intézkedések értékelése és elemzése alapján végrehajtott válaszintézkedéseket.

g) az EIR biztonsági állapotáról rendszeres időközönként történő jelentés a kijelölt személyeknek.

II.6.7. Folyamatos felügyelet – Kockázatmonitorozás (*)

A Hivatal biztosítja, hogy a kockázatmonitorozás szerves része legyen a folyamatos felügyeleti stratégiának, amely a következőket tartalmazza:

a) a hatékonyság ellenőrzését;

b) a megfelelés ellenőrzését; és

c) a változások nyomon követését.

II.6.8. Belső rendszerkapcsolatok (*)

A Hivatal engedélyezési eljáráshoz köti a belső EIR-jei összekapcsolását.

Minden belső kapcsolat esetében dokumentálja az interfész jellemzőit, a biztonsági követelményeket, továbbá a kommunikációban részt vevő információ jellegét.

Meghatározott feltételek teljesülése esetén megszünteti a belső rendszerkapcsolatokat.

2 évente felülvizsgálja minden belső kapcsolat további szükségességét.

II.7. KONFIGURÁCIÓKEZELÉS

A technológiai vhr **KONFIGURÁCIÓKEZELÉS** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.7.1. Szabályzat és eljárásrendek

A Hivatal konfigurációkezelési szabályzatát az IBSZ jelen fejezete tartalmazza.

II.7.2. Alapkonfiguráció

A Hivatal valamennyi elektronikus információs rendszeréhez elkészíti az alapkonfigurációt, amelyet dokumentált formában biztonságos helyen tárolni szükséges.

A dokumentációnak minimálisan a következő elemeket kell magában foglalnia: a munkaállomásokra, kiszolgálókra, a hálózati eszközökre és egyéb mobil eszközökre telepített operációs rendszerek és egyéb szoftverek verzióit, patch szintjét, továbbá az egyes szoftverkomponensek biztonságosnak ítélt konfigurációs beállításait.

Vázolni kell az érintett EIR elhelyezkedését a logikai topológiában.

Az egyes elektronikus információs rendszerek alapkonfigurációját a rendszergazda évente felülvizsgálja, és a módosításokat átvezeti.

II.7.3. Biztonsági hatásvizsgálatok (*)

A változtatás megkezdése előtt az IBF-nek egy előzetes kockázatelemzéssel és a biztonsági funkciók tesztelésével kell biztosítania a változtatás éles környezetre ható kockázatainak

minimalizálását. A kockázatelemzésnek ki kell terjedni minden olyan lényeges elemre, amely rávilágíthat a változtatás következtében bekövetkező biztonsági problémákra.

II.7.4. A változtatásokra vonatkozó hozzáférés korlátozások

Az EIR-ek változtatását a Hivatal rendszergazdái jogosultak végrehajtani.

II.7.5. Konfigurációs beállítások (*)

A vizsgált rendszer működtetése során csak jóváhagyott hardver és szoftver elemek használhatók, melyek a rendszer rendszerdokumentációjában szerepelnek. A rendszer minden egyes eleméhez a konfigurációs beállítások elvégzését, annak dokumentálását végre kell hajtani. Minden egyes módosítást, amelyek a konfiguráció beállításokhoz köthetőek, megfelelően dokumentálni kell.

A kötelező, jóváhagyott konfigurációs beállításokat az IBF az éves ellenőrzési tervében foglaltak szerint, a rendszerdokumentációban foglaltak alapján ellenőrzi.

II.7.6. Legszűkebb funkcionalitás (*)

A Hivatal elektronikus információs rendszereiben csak a szükséges portokat, protokollokat és szolgáltatásokat szabad engedélyezni. Az engedélyezett portokat, protokollokat és szolgáltatásokat dokumentálni kell a rendszer alapkonfigurációjában.

A munkaállomások és a kiszolgálók alapkonfigurációjának a kialakításakor figyelembe kell venni a nemzetközi „Center for Internet Security” szervezet ajánlásait. Ennek érdekében hardening guide-okat kell kidolgozni és beállítani az EIR-eket alkotó szoftverkomponensek esetében.

II.7.7. Rendszerelem leltár

Az elektronikus információs rendszerek valamennyi hardver/szoftver eleméről a rendszergazdának nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a kiszolgálók, a munkaállomások és a hálózati eszközök pontos és naprakész hardver és szoftver konfigurációját, az elhelyezkedésüket és az értük felelős személy nevét.

II.7.8. A szoftver használat korlátozásai

A Hivatalnál kizárólag a Jegyző által engedélyezett, jogtiszta, a megfelelő licence-szel rendelkező szoftvereket lehet használni.

Az alkalmazott szoftverekről leltárt kell vezetni.

Szabad vagy nyílt forráskódú szoftverek használatbavételét a Jegyző engedélyezi. Ezen szoftvereket használatba vétel előtt biztonságos körülmények között tesztelni kell.

A másolatok és szétosztások ellenőrzése érdekében a telepítőkészleteket és a licenceket tartalmazó dokumentumokat páncélszekrényben kell tárolni és a hozzáféréseket ellenőrizni kell.

A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni.

II.7.9. A felhasználó által telepített szoftverek

A felhasználók semmilyen alkalmazást (beleértve a csupán másolással telepíthető alkalmazásokat is) nem telepíthetnek a munkaállomásaikra. A rendszerprogramok, illetve a felhasználói alkalmazások telepítését a kiszolgálókra és munkaállomásokra csak a rendszergazda végezheti el.

A felhasználók munkaállomásain telepített alkalmazások megfelelőségét az IBF szúrópróba szerűen ellenőrzi.

II.8. KÉSZENLÉTI TERVEZÉS

A technológiai vhr **KÉSZENLÉTI TERVEZÉS** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.8.1. Szabályzat és eljárásrendek

A Hivatal Üzletmenet-folytonossági szabályzatát az IBSZ jelen fejezete tartalmazza.

II.8.2. Üzletmenet-folytonossági terv

Az IBF-nek az érintett területek bevonásával ki kell dolgoznia és a Jegyzővel jóvá kell hagyatnia az elektronikus információs rendszerekre vonatkozó ügymenet-folytonossági tervet (továbbiakban: ÜFT).

Az ÜFT-ben meg kell határozni azokat a folyamatokat, melyeket EIR-ek segítségével végeznek.

Az ÜFT-ben – az adatgazdák és folyamatgazdák bevonásával - meg kell határozni az EIR-ek RTO és RPO értékeit.

A folyamatos működés tervezésére vonatkozó tevékenységeket össze kell hangolni a biztonsági események és vészhelyzeti/katasztrófa helyzetek kezelésével.

A tervezés során meg kell határozni a Hivatal által biztosítandó szolgáltatásokat és alapfunkciókat, valamint az ezekhez kapcsolódó és a Hivatal részéről elvárt vészhelyzeti követelményeket.

Meg kell határozni az elektronikus információs rendszer kiesése esetére a helyreállítási feladatokat, a helyreállítási prioritásokat és azok mértékét.

Ki kell jelölni a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket.

Az ügymenet-folytonosságot úgy kell kialakítani, hogy az biztosítsa a Hivatal által előzetesen definiált alapszolgáltatások fenntartását, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is.

Ki kell dolgozni a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

II.8.3. A folyamatos működésre felkészítő képzés (*)

Évente dokumentált módon (jegyzőkönyvvel és jelenlétivel igazolva) folyamatos működésre felkészítő képzést kell tartani, melynek során képezni kell a felhasználókat az ÜFT-ben foglaltakról. A képzést az IBF-nek kell megtartania. A képzésen a részvétel kötelező.

II.8.4. Az elektronikus információs rendszer mentései

Az elektronikus információs rendszerek és az azokban kezelt adatok az adatgazdák és a jogszabályok által elvárt, megfelelő rendelkezésre állásának biztosítása érdekében mentési eljárásrendet kell kidolgozni a következők figyelembevételével:

Rendszeres mentéseket kell készíteni valamennyi EIR-ről és az azokban kezelt adatokról.

A mentések során a következő adatfajták mentését kell biztosítani:

a) felhasználói szintű adatok (ügyviteli adatok);

b) rendszerszintű információk;

c) naplóinformációk;

d) a rendszerrel kapcsolatos dokumentációk.

A mentési stratégiát az ÜFT-ben kell rögzíteni. A mentési stratégiát az EIR-ek RTO és RPO értékei alapján kell kialakítani.

Biztosítani kell a háttérkörnyezetet, annak érdekében, hogy a lényeges adatok és szoftverek esetleges adathordozó hiba, az elektronikus információs rendszerek összeomlása vagy megsemmisülése esetén visszaállíthatóak legyenek.

A mentési eljárásrendet úgy kell kialakítani, hogy az egyrészt megfeleljen az üzembiztonsági elvárásoknak, másrészt a Hivatal részére elfogadható védelmet nyújtson az esetlegesen előforduló hibák ellen.

Az ügymenet folytonosság fenntartása érdekében a mentéseket tartalmazó adathordozókat szerverhelyiségtől elkülönítve, páncélszekrényben kell tárolni.

II.8.5. Az elektronikus információs rendszer helyreállítása és újraindítása

Az ügymenet-folytonosság tervezése során ki kell dolgozni az elektronikus információs rendszerek helyreállítási terveit, melyeknek a katasztrófahelyzetek kezelésére vonatkozóan a következőket kell tartalmazniuk:

a) katasztrófát követő helyreállítandó célállapot;

b) a katasztrófa események definíciója;

c) a katasztrófa tényét eldöntő, a folyamat inicializálásáért felelős személyt, személyeket;

d) a helyreállítási terv hatóköre;

e) a megelőzés érdekében végzett tevékenységeket;

f) felkészülés a katasztrófa elhárítására;

g) katasztrófa esetén végrehajtandó tevékenységek;

h) elektronikus információs rendszerek vészleállításának és újraindításának folyamatát leíró dokumentumot;

i) a helyreállítási terv tesztelése, karbantartása.

Az elektronikus információs rendszerekre vonatkozó helyreállítási tervek elkészítéséről, teszteléséről és folyamatos karbantartásáról a rendszergazda gondoskodik. A terv készítési tevékenységeket az IBF-nek információbiztonsági szempontból támogatnia és évente ellenőriznie kell.

A terveket minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs infrastruktúra (pl.: új elektronikus információs rendszer bevezetése, új nagyteljesítményű hardverelemek változása).

A rendszergazdának - mindezeken túl - gondoskodnia kell az elektronikus információs rendszer helyreállításához szükséges mentések meglétéről, elérhetőségéről.

II.9. AZONOSÍTÁS ÉS HITELESÍTÉS

A technológiai vhr **AZONOSÍTÁS ÉS HITELESÍTÉS** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.9.1. Szabályzat és eljárásrendek

A Hivatal azonosítási és hitelesítési szabályzatát az IBSZ jelen fejezete tartalmazza.

II.9.2. Azonosítás és hitelesítés

Valamennyi EIR-nek egyedileg kell azonosítania és hitelesítenie a Hivatal valamennyi felhasználóját és a felhasználók által végzett tevékenységeket.

Ennek érdekében egyénre szóló felhasználói azonosítókat kell képezni, a csoportos azonosítók használata nem engedélyezett.

II.9.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése (*)

A privilegizált felhasználói fiókok hálózati hozzáférésekor többtényezős azonosítást és hitelesítést kell alkalmazni, oly módon, hogy a hálózati bejelentkezés során tudás (hálózati azonosító és jelszó) mellett birtoklás (hard vagy soft token) alapú azonosítást és hitelesítést is alkalmaz a Hivatal.

A többtényezős hitelesítést távoli hozzáférések során is alkalmazni kell.

II.9.4. Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – Visszajátszás elleni védelem (*)

Az EIR-ek azonosítási és hitelesítési folyamatai során a jelen IBSZ *{II.9.7.* A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés (*)*}* fejezetében előírt algoritmusokat kell alkalmazni, melyek biztosítják a visszajátszás elleni védelmet.

II.9.5. Azonosító kezelés

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat a rendszergazda hozza létre. Az azonosítók létrehozását az adatgazdák engedélyezik Az azonosítók ismételt felhasználása tilos.

90 nap inaktivitás után az azonosítókat a rendszergazdának le kell tiltania.

A fentiek három havi rendszerességgel történő végrehajtása a rendszergazdák feladata.

Az azonosítókat évente felül kell vizsgálni. A felülvizsgálatot a rendszergazdák végzik el.

II.9.6. A hitelesítésre szolgáló eszközök kezelése

A jelszavak a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszernek hatékonyan és interaktívan kell biztosítania a megfelelő színvonalú jelszavak használatát.

A Hivatal jelszókezelő rendszere:

a) tegye lehetővé a felhasználók számára jelszavuk kiválasztását és megváltoztatását;

b) kényszerítse ki az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor;

c) kényszerítse ki a megfelelő minőségű jelszavak használatát;

d) kényszerítse ki a jelszóváltoztatást;

e) tiltsa meg a korábban használt jelszavak ismételt felhasználását;

f) beíráskor ne jelenítse meg a jelszavakat a képernyőn;

g) a jelszó állományokat rejtjelezve tárolja;

h) változtassa meg a szállító alapértelmezett jelszavát a szoftver installálása után.

Jelszógondozási folyamattal kell a jelszavak kiosztását ellenőrizni, úgy, hogy:

a) szükség esetén a felhasználók kötelezhetők arra, hogy nyilatkozatban vállalják a számukra kiadott, vagy általuk képzett jelszavaik titokban tartását;

b) biztosítani, hogy a kezdeti jelszavak is biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

a) a jelszó legalább 12 karakter hosszú legyen, és - ahol műszakilag az megvalósítható - törekedni kell arra, hogy tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

b) a jelszavakat 2 napon belül nem szabad megváltoztatni;

c) a jelszavakat 365 naponta havonta meg kell változtatni;

d) az előző jelszavak újra használatát 12 alkalomig kerülni kell;

e) biztosítani kell a jelszó megváltoztatásának a lehetőségét, amennyiben a felhasználó kezdeményezi, illetve ha felmerül a jelszó kompromittálódása.

f) 5 sikertelen bejelentkezési kísérlet esetére 30 percre zárolja a fiókot és a számlálót 30 perc után nullázza.

II.9.6.1. Technikai azonosítók kezelése

A technikai azonosítók elkülönített úton történő kezelését a jelen fejezetben foglaltak szerint kell megvalósítani:

A technikai azonosítókat a rendszergazda hozza létre. A technikai azonosítóknak nem adható automatikusan rendszergazda jog, törekedni kell a „szükséges, minimális jogok elve” alapján a minimális jog biztosítására.

Az azonosítók létrehozásánál biztosítani kell a nevükben futó alkalmazások, szolgáltatások egyedi azonosítását és hitelesítését a következő névkonvenció alapján: _svc_”futó szolgáltatás rövid neve”.

A technikai azonosítók jelszavait jelszógenerátorral kell képezni, a jelszó hossza minimum 20 karakter legyen és feleljen meg a bonyolultsági kritériumnak.

A jelszavakat lezárt borítékban és páncélszekrényben vagy szabványos, kriptográfiai algoritmussal őrzött jelszókonténerben kell tárolni. A jelszókonténer mester jelszavát lezárt borítékban, páncélszekrényben kell tárolni

Meg kell változtatni a jelszót, ha felmerül a jelszó kompromittálódása.

II.9.6.2. Rendszergazdai jelszavak kezelése

A rendszergazdai jelszavak képzéséhez az alábbi szabályokat kell betartani:

a) A jelszó legalább 15 karakter hosszú legyen, és - ahol műszakilag az megvalósítható - törekedni kell arra, hogy tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is.

b) A jelszavakat két napon belül nem szabad megváltoztatni.

c) Az előző jelszavak újra használatát 24 alkalomig kerülni kell.

d) A jelszavakat 6 havonta meg kell változtatni.

e) Biztosítani kell a jelszó megváltoztatásának a lehetőségét, amennyiben a felhasználó kezdeményezi, illetve ha felmerül a jelszó kompromittálása.

II.9.7. A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés (*)

Törekedni kell arra, hogy az EIR-ek azonosítás és hitelesítés során címtár alapú hitelesítést (active directory integrált) alkalmazzanak.

Helyi azonosítás és hitelesítés során csak olyan jelszótárolási módszert lehet alkalmazni, amely nem tárolja a jelszót nyílt formában. A jelszavak tárolását a következő mértékadó dokumentumokban biztonságosnak minősített algoritmussal (pl.: Argon2id, bcrypt) kell megvalósítani.

Jelszavak tárolását a következő mértékadó dokumentumban biztonságosnak mondott algoritmussal kell megvalósítani.

a) NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management;

b) Open Web Application Security Project Password Storage Cheat Sheet.

A megfelelő algoritmus kiválasztásába be kell vonni az IBF-et.

II.9.8. Hitelesítési információk visszajelzésének elrejtése

Az illetéktelen hozzáférések elkerülése érdekében olyan hitelesítési módszereket kell alkalmazni, amely a beütött jelszavak karaktereit valamilyen helyettesítő karakterrel ábrázolja (pl.: csillag karakter).

II.9.9. Hitelesítés kriptográfiai modul esetén

A Hivatal nem alkalmaz kriptográfiai modult az azonosítási és hitelesítési folyamatai során.

II.9.10. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Az elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie az érintett szervezeten kívüli felhasználókat, illetve a tevékenységüket.

II.9.11. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – Meghatározott azonosítási profilok használata

A szervezeten kívüli felhasználók esetében meg kell határozni azokat a profilokat melyek alapján a felhasználói fiókok létrehozhatóak.

II.9.12. Újrahitelesítés (*)

Az azonosítási és hitelesítési során 8 órás tétlenség után újra kell hitelesítenie magát a felhasználónak.

II.10. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A technológiai vhr **BIZTONSÁGI ESEMÉNYEK KEZELÉSE** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.10.1. Szabályzat és eljárásrendek

A Hivatal biztonsági eseménykezelési szabályzatát az IBSZ jelen fejezete tartalmazza.

II.10.2. Biztonsági események meghatározása

Információbiztonsági eseménynek minősül minden 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, így különösen:

a) a szolgáltatás, a berendezés vagy az eszközök elvesztése;

b) a rendszer hibás működése vagy túlterhelések (DoS-támadás);

c) emberi hibák;

d) a szabályzatoknak vagy irányelveknek való nem megfelelés;

e) a fizikai biztonsági rendelkezések megsértése;

f) nem ellenőrzött rendszerbeli változások;

g) a szoftver vagy hardver hibás működése;

h) hozzáférési előírások megsértése;

i) kártékony kód általi fertőzés;

j) a nem teljes, vagy nem pontos működési adatokból eredő hibák;

k) a bizalmasság és sértetlenség megsértése;

l) az elektronikus információs rendszerrel való visszaélés.

II.10.2.1. Biztonsági események kategorizálása

A Hivatal az elektronikus információs rendszereit érintő biztonsági eseményeket két kategóriába sorolja:

a) Súlyos biztonsági esemény;

b) Enyhébb fokozatú biztonsági esemény.

II.10.2.1.1. Súlyos biztonsági esemény

A Hivatalban a következők számítanak súlyos biztonsági eseménynek:

a) Egynél több, vagy a Hivatal összes elektronikus információs rendszerét érintő biztonsági esemény;

b) A bekövetkezett kár mértéke alapján a társadalmi-politikai hatás jelentős;

c) Személyes adatok illetéktelen kézbe kerülése feltételezhető;

d) Jogszabály által védett adatok illetéktelen kézbe kerülése feltételezhető.

II.10.2.1.2. Enyhébb fokozatú biztonsági esemény

A Hivatalban a következők számítanak enyhébb fokozatú biztonsági eseménynek:

a) Nem kritikus elektronikus információs rendszer adat bizalmasságának sértetlensége vagy rendelkezésre állása sérül;

b) Az ügymenetet jelentősen nem befolyásoló, elektronikus információs rendszer rendelkezésre állása sérül.

II.10.3. Képzés a biztonsági események kezelésére (*)

Az általános biztonságtudatossági képzés részévé kell tenni a biztonsági események kezelésével összefüggő ismereteket, így különösen

a) a biztonsági esemény fogalma;

b) biztonsági események fajtái;

c) teendők biztonsági esemény esetén;

d) biztonsági események dokumentálása;

e) tájékoztatás közreműködési kötelezettségről a biztonsági események kivizsgálása során;

f) eljáró szervek biztonsági eseménye esetén eljáró szervek, hatóságok feladatainak ismertetése;

g) szükséges javító intézkedések megtétele biztonsági események kivizsgálása után.

II.10.4. Biztonsági események kezelése

A biztonsági eseményeket a jelen fejezetben foglaltak alapján kell kezelni.

II.10.4.1. Észlelés

Az észlelés magában foglalja a számítástechnikai rendszerek, hálózatok és incidens jelentési mechanizmusok, például jegyrendszerek vagy e-mail elosztások figyelését a rendellenes és esetleg rosszindulatú események miatt. Ez a fázis magában foglalja egy megfelelő alapinformáció összegyűjtését is, amely segíti az elsősegélynyújtókat az esemény megértésében és kivizsgálásában.

Célok:

a) Bejelentés fogadása, rögzítése.

b) Azonosítani kell az érintett rendszerelemeket.

c) Össze kell gyűjteni az incidenssel kapcsolatos összes rendelkezésre álló információt.

d) Azonosítani kell az érintett rendszerben kezelt adatok típusait.

e) Meg kell becsülni az incidens súlyosságát az adatosztályozás és az incidens típusa/súlyossága alapján.

A biztonságot érintő eseményekről, a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és a rendszergazdát.

A biztonságot érintő eseményekről szóló jelentések elkészítésére a jelen IBSZ *{5. számú melléklet – Biztonsági események jelentése}* mellékletében található űrlapot kell használni.

II.10.4.2. Elszigetelés

A biztonsági eseményben érintett rendszerelemeket azonnal el kell különíteni a többi, éles üzemben működő rendszerelemektől (le kell választani a hálózatról) a biztonsági esemény elhárítása és a biztonsági esemény kivizsgálásának időtartamára.

A korlátozás magában foglalja a számítási környezet módosítását az aktív fenyegetések mérséklése érdekében a jelenleg ismert információk alapján.

Az elszigetelési tevékenység magában foglalhatja a rendszerek elkülönítését karanténban vagy VLAN-okon keresztül, a tűzfal hozzáférés-szabályozásának módosítását a további kommunikáció vagy adatszivárgás megakadályozása érdekében, vagy olyan gyorsjavítások vagy víruskereső definíciófrissítések terjesztését, amelyek megakadályozzák egy aktív rosszindulatú programfertőzés tovább terjedését.

II.10.4.3. Megszűntetés

A felszámolás magában foglalja a rendszer vagy rendszerek eltávolítását a hálózatból. Ez szükségessé teheti a hálózati port kikapcsolását és/vagy az érintett rendszer vagy rendszerek leállítását.

Az incidens súlyosságától és típusától függően a kiberbiztonsági incidenskezelő Hivatal dönthet úgy, hogy figyelemmel kíséri az érintett rendszereket, hogy jobb megértést kapjon, mielőtt blokkolna egy folyamatban lévő támadást. Ez azzal az előnnyel járhat, hogy a csapat több információt gyűjthet a támadásról, ami jobban megértheti a támadás teljes terjedelmét, célját és eredetét. Azonban olyan körülmények között, amikor a bizalmas információk aktívan kiszivárognak, a kritikus rendszerek veszélyben vannak, vagy emberéletek vannak veszélyben, a támadás megállítása a legfontosabb.

Nyomon kell követni az adott eseménytípusra vonatkozó megfelelő eljárási útmutatót, hatósági ajánlást.

Meg kell határozni a támadás hatásait és azonosítani kell az összes lehetséges információt, rendszert és erőforrást, amely kompromittálódhatott.

Listát kell készíteni azokról az eszközökről, EIR-ekről, amelyekről adatokat gyűjthetett a támadó.

Felszámolási stratégia kidolgozása a fenyegetés(ek) hatékony és eredményes eltávolításának biztosítására.

II.10.4.4. Helyreállítás

A helyreállítás magában foglalja a számítási rendszerek és hálózatok újraképezését és normál működésbe való visszaállítását, miután a fenyegetést a környezetből alaposan felszámolták. A helyreállítási tevékenység, például az adatok visszaállítása biztonsági másolatokból, a szolgáltatások új kiszolgálókra való migrálása vagy a megtisztított rendszerek visszaküldése az éles hálózatokhoz.

Miután maga a probléma megoldódott, a Hivatalnak vissza kell állítania a normál üzleti működést. Ez magában foglalja az incidens által okozott károk visszafordítását és a reagálást. Például minden elveszett adatot vissza kell állítani a biztonsági másolatokból, és el kell távolítani a válasz során bevezetett ideiglenes tűzfalszabályokat vagy útválasztó ACL-eket.

Minden érintett rendszert teljesen újjá kell építeni és javítani kell, és felül kell vizsgálni a javítási eljárásokat, hogy biztosítsák azok megfelelő végrehajtását. Ennek célja, hogy megoldja a mögöttes problémát, és megakadályozza az incidens megismétlődését.

Helyreállítás – megvalósítandó célok:

a) Szükség szerint törölni és újra kell telepíteni az érintett rendszert.

b) Értesíteni kell az érintett feleket, hogy az esemény a helyreállítási fázisban van.

c) Adatok visszaállítása biztonsági másolatokból.

d) Ideiglenes tűzfalszabályok visszaállítása, ideiglenes rendszermódosítások helyreállítása, amelyek szükségesek voltak az elszigeteléshez.

Újra kell csatlakoztatni az érintett rendszert a hálózathoz.

II.10.5. A biztonsági események nyomonkövetése (*)

Nyilvántartást kell vezetni biztonsági eseményekről a későbbi vizsgálatok lefolytatása érdekében.

A Nyilvántartást az IBF vezeti.

A nyilvántartásban a következőket kell rögzíteni:

a) biztonsági esemény megnevezése;

b) biztonsági esemény leírása;

c) biztonsági esemény bekövetkezésének dátuma;

d) érintett EIR-ek;

e) EIR-ek leállásának részletei;

f) biztonsági esemény súlyossága;

g) okozott kár leírása;

h) biztonsági esemény elhárítása érdekében tett intézkedések leírása;

i) biztonsági esemény elhárításának dátuma.

II.10.6. A biztonsági események jelentése

A biztonságot érintő eseményekről, a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és a rendszergazdát.

A biztonságot érintő eseményekről szóló jelentések elkészítésére a jelen IBSZ *{5. számú melléklet – Biztonsági események jelentése}* mellékletében található űrlapot kell használni.

Amennyiben a rendszergazda úgy ítéli meg, hogy a bejelentett probléma biztonsági eseményre utal, úgy jelentenie kell az IBF-nek.

Biztonsági esemény esetén az IBF látja el a biztonságiesemény-kezelési megbízott feladatait.

Az IBF-nek haladéktalanul jelentenie kell a biztonsági eseményt a kiberbiztonsági incidenskezelő Hivatal részére.

Az IBF-nek csatolnia kell a bejelentéshez a biztonsági eseményhez kapcsolódó valamennyi bizonyítékot.

Az IBF-nek és a Hivatalnak együtt kell működnie a kiberbiztonsági incidenskezelő Hivatal és a Hivatal által javasolt intézkedéseket végre kell hajtania.

Az IBF-nek kivizsgálást kell kezdeményeznie a beérkezett jelentés alapján és javaslatot kell tennie a Jegyző részére az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.

Amennyiben a biztonsági esemény igazoltan a szabályok megsértéséből adódik, úgy az IBF-nek javaslatot kell tennie a Jegyző részére a fegyelmi eljárások lefolytatása érdekében.

II.10.7. Segítségnyújtás a biztonsági események kezeléséhez (*)

Az IBF az IBSZ jelen fejezetében foglaltak alapján közreműködik a biztonsági események kezelésében.

II.10.8. Biztonsági esemény-kezelési terv (*)

A Hivatal biztonsági esemény-kezelési tervét a IBSZ jelen fejezete tartalmazza.

II.11. KARBANTARTÁS

A technológiai vhr **KARBANTARTÁS** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.11.1. Szabályzat és eljárásrendek

A Hivatal karbantartási szabályzatára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.11.2. Szabályozott karbantartás

A Hivatal az EIR-ek karbantartását a jelen fejezet szerint hajtja végre.

II.11.2.1. A karbantartások engedélyezése

A tervezett karbantartásokat dokumentált formában a Jegyző engedélyezi. Amennyiben ez az elektronikus információs rendszerek leállításával jár, akkor a felhasználókat a karbantartás megkezdése előtt legalább 1 héttel értesíteni szükséges.

II.11.2.2. A karbantartások dokumentálása, nyilvántartása

Az elvégzett munkákat jegyzőkönyvezni kell, valamint a karbantartás tényét karbantartási nyilvántartásban kell dokumentálni, illetve nyilvántartani. A nyilvántartásba a következő adatokat kell minimálisan rögzíteni:

a) az elvégzett karbantartás megnevezése;

b) az érintett eszközök, szoftverek, elektronikus információs rendszerek;

c) a karbantartás engedélyezője;

d) a karbantartás elvégzője;

e) a karbantartás dátuma;

f) leállási idő (ha volt ilyen).

a Jegyzőkönyveket csatolni kell a karbantartási nyilvántartáshoz.

II.11.2.3. A karbantartások ütemezése

Éves karbantartási tervet kell készíteni, melyben meg kell tervezni a karbantartások ütemezését. A terv elkészítése a rendszergazda, a terv jóváhagyása a Jegyző feladata.

II.11.2.4. Kiszállítás

Amennyiben az adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor a jelen IBSZ *{II.12.4. Az infokommunikációs eszközök biztonságos újrahasznosítása, mások rendelkezésére bocsátása, selejtezése}* fejezetben leírtak szerint kell eljárni. A kiszállítást a rendszergazda engedélyezi.

II.11.2.5. A karbantartás ellenőrzése

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági teszteket kell végezni, melynek eredményét rögzíteni kell a karbantartási nyilvántartásban. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe.

II.11.3. Távoli karbantartás

A Hivatalban nem engedélyezett az EIR-ek távoli karbantartása.

II.11.4. Karbantartó személyek

Abban az esetben, ha saját erőből a karbantartás nem végezhető el, akkor a rendszergazda kezdeményezi a Jegyzőnél külső fél (alvállalkozó) megbízását.

Karbantartási tevékenységet csak olyan külső fél végezhet, aki érvényes szerződéssel rendelkezik, a titoktartási nyilatkozatot aláírta és dokumentált formában megismerte a Hivatal vonatkozó információbiztonsági előírásait.

A karbantartást végző, külső felekről nyilvántartást kell vezetni, melynek minimálisan a következőket kell tartalmaznia:

a) szervezet megnevezése;

b) szerződésszám;

c) szerződés időtartama;

d) szerződéses kapcsolattartó neve, elérhetősége;

e) karbantartás végzők neve, elérhetősége;

f) szerződés tárgya, hatálya (mely rendszerelemre terjed ki).

Külsős szerződő fél munkavégzése esetén a rendszergazda biztosítja a folyamatos felügyeletet a karbantartás során.

A külső féllel kötött szerződébe kell foglalni, hogy a karbantartást felügyelők jogosultak kérni a karbantartást végző személy személyazonosságának igazolását, illetve hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

II.12. ADATHORDOZÓK VÉDELME

A technológiai vhr **ADATHORDOZÓK VÉDELME** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.12.1. Szabályzat és eljárásrendek

A tudatossági és képzési eljárásrendet az IBSZ jelen fejezete tartalmazza.

II.12.2. Hozzáférés az adathordozókhoz, adathordozók használata

A Hivatalnál csak a Hivatal tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését a rendszergazdához kell benyújtania a szervezeti egység vezetőjének.

Az adathordozók kiadását az érintett szervezeti egység vezetője engedélyezi.

Az eszközhasználatot, a Hivatal elektronikus információs rendszereihez történő csatlakoztatása után, a Hivatal minden előzetes értesítés nélkül figyelheti, monitorozhatja.

Otthoni munkavégzés és bármilyen más célból bármilyen adatot elektronikus levélben vagy egyéb más eszközön (pl.: Pen drive) a Hivatal informatikai infrastruktúrájából kijuttatni csak az Adatgazda írásos engedélyével szabad. Az adatok kivitelét az Adatgazdának vagy a szervezeti egység vezetőjének kell engedélyeznie, minden esetben írásos formában.

A Hivatal az adathordozók használatát információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

II.12.3. Adathordozók tárolása

A Hivatal elektronikus információs rendszereinek kiszolgáló oldali adathordozóit a szerverhelyiségben kell tárolni. A szerverhelyiség fizikai védelmét a jelen *IBSZ {II.13. Fizikai és környezeti védelem }* fejezetében foglaltaknak megfelelően kell kialakítani.

A felhasználók részére kiosztott mobil adathordozókat használaton kívül zárható irodabútorban kell tárolni.

II.12.4. Az infokommunikációs eszközök biztonságos újrahasznosítása, mások rendelkezésére bocsátása, selejtezése

II.12.4.1. Újrahasznosítás

Infokommunikációs eszközök újrahasznosítása előtt a következők végrehajtása szükséges:

a) A rajtuk tárolt adatokat, az adat érzékenységének megfelelő erősségű, helyreállíthatatlanságot garantáló, logikai vagy fizikai törléssel törölni kell.

b) A törlést az adattárolón lévő adatok gazdájának jóvá kell hagynia.

c) Garanciális eszközök esetén, ha az eszköz hibája miatt az adatok törlésére nincs mód, az IBF dönt az eszköz cserére történő kiadhatóságáról, vagy megsemmisítéséről.

Az adathordozókon tárolt adatok törlését, az adat *{NIST 800-88 Rev1 - Guidelines for Media Sanitization.}* szabványban foglaltak szerinti minősítési kategóriájának, illetve az újra felhasználás és mások rendelkezésre bocsájtásának függvényében logikai törléssel, purgálással vagy fizikai megsemmisítéssel kell elvégezni.

A Hivatali adatokat tartalmazó infokommunikációs eszközök harmadik fél részére történő átadása újra felhasználás céljából - a fentiek végrehajtásától függetlenül információbiztonsági szempontból - nem engedélyezett, egyedi esetekről a Jegyző az IBF bevonásával dönt.

II.12.4.2. Selejtezés

Infokommunikációs eszközök selejtezése előtt a Hivatal Selejtezési Szabályzatában foglaltakon túl, még működőképes eszköz esetén a rajtuk tárolt adatokat helyreállíthatatlanságot garantáló logikai törléssel (pl.: Eraser) a rendszergazda útján törölni kell, valamint függetlenül az eszköz működőképességétől, megfelelő tanúsítvánnyal rendelkező adatmegsemmisítéssel foglalkozó szakértő bevonásával fizikai rongálással vagy megsemmisítéssel kell gondoskodni az eszközökön tárolt adatok visszaállíthatatlanságáról.

Az adatok megfelelő módon történő eltávolításáért a rendszergazda a felelős. Az adatok eltávolítását jegyzőkönyvezni kell.

II.12.5. A hordozható infokommunikációs eszközök védelme

A hordozható infokommunikációs eszközök használata során a munkaállomásokra vonatkozó előírásokon kívül az alábbi védelmi szabályokat kell betartani:

a) Mechanikai és használati sérülések elkerülése érdekében követni kell a géphez kapott használati útmutatót.

b) Cserélhető kártyák behelyezésénél, és eltávolításánál szintén a használati utasítást kell követni.

c) A mobilitás és a kis méret miatt, a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek, emiatt nem szabad őrizetlenül hagyni autóban, szállodai szobában.

II.12.6. Mobil infokommunikációs eszközök ellopása esetén

Mobil infokommunikációs eszközök ellopása esetén:

a) az ellopás tényét a lehető leggyorsabban jelenteni kell az érintett vezetőnek és az IBF-nek;

b) értesíteni kell a rendőrséget;

c) értesíteni kell a szálloda vezetését, ha az eszközt a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;

d) valamennyi rendőrségi jelentést meg kell őrizni és a Jegyző részére át kell adni.

II.12.7. Infokommunikációs eszköz elvesztése

Bármely infokommunikációs eszköz eltűnését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek és az IBF-nek, valamint tájékoztatni kell őket arról, hogy az eszköz tartalmaz-e bárminemű érzékeny információt. (Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve.)

II.13. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

A technológiai vhr **FIZIKAI ÉS KÖRNYEZETI VÉDELEM** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.13.1. Szabályzat és eljárásrendek

A tudatossági és képzési eljárásrendet az IBSZ jelen fejezete tartalmazza.

II.13.2. Alapelvek

Az elektronikus információs rendszer fizikai környezetének kialakítása, működtetése és használata során az általános biztonsági előírások szerint kell eljárni, az alábbiak szerint:

a) az elektronikus információs rendszereket fizikailag védett, biztonságos helyre kell telepíteni, és a környezetet a berendezések gyártói által megadott fizikai feltételek szerint kell kialakítani, fenntartani;

b) a környezeti fizikai feltételeket (hőmérséklet, páratartalom, áramszolgáltatás stb.) folyamatosan ellenőrizni kell;

c) a megbízható működés biztosítása céljából a körülményeknek megfelelő legfontosabb klímatechnikai, épületgépészeti, áramellátó tartalékberendezésekről gondoskodni kell.

II.13.3. A területek fizikai biztonsági követelményei

II.13.3.1. Fizikai biztonság védősávja

A védett helyiségeket, illetve területeket a fenyegetettség és kockázat mértéke szerint biztonsági zónákba kell besorolni. Héjszerű, többlépcsős fizikai védelmet kell kialakítani.

A jelen IBSZ *{I.2.2. Tárgyi hatály}* pontja alá eső területeket az alábbi kategóriák egyikébe kell besorolni:

a) belső terület;

b) védett terület;

c) érzékeny terület.

További védett terület kategóriákat az IBF határozhat meg.

II.13.3.2. Belső terület

Belső területnek tekintendők a Hivatal bejárata utáni, közös használatú helyiségei és folyosói.

A belső terekben infokommunikációs eszközök nem telepíthetők, a kivételek jóváhagyása az IBF feladata.

II.13.3.3. Védett terület

Védett terület valamennyi iroda és tárgyaló helyiség.

A védett területeken a következő védelmi intézkedéseket kell alkalmazni:

a) A kulcsokat nem szabad nyilvános, idegenek számára is könnyen hozzáférhető helyen tárolni.

b) A fénymásoló és nyomtató berendezéseket, a fax készülékeket védett területen belül kell elhelyezni. Gondoskodni kell arról, hogy a belső területen elhelyezett eszköz esetében csak egyedi azonosítás és hitelesítés után lehessen a nyomtatást az eszközön elindítani;

c) A dokumentumok tárolása védett területen történjen.

d) Azokban az időszakokban, amikor a helyiségek felügyelet nélkül maradnak, az ajtókat és ablakokat zárva kell tartani.

e) A védett területek bejárati ajtajában a kulcsokat nem szabad a zárban hagyni, illetve ha az ajtó nyitva van, a helyiséget nem szabad őrizetlenül hagyni.

f) Munkaidőn kívül, amikor az épületben senki sem tartózkodik a belső és a védett területeken, elektronikus riasztórendszert kell alkalmazni.

g) Ügyfelet és más külsős személyt nem szabad felügyelet nélkül hagyni.

II.13.3.4. Érzékeny terület

Érzékeny terület a Hivatal

a) szerverszobája és

b) a strukturált kábelezés rendező központjai.

Az érzékeny területekre vonatkozóan a következő védelmi intézkedéseket kell megvalósítani:

a) Az érzékeny területek elérésére a Jegyző, a rendszergazda és az IBF jogosultak. Minden más személy részére csak a Jegyző engedélyezheti a belépést.

b) Látogatók belépése az érzékeny területre csak hivatali célból, ellenőrzötten és kísérővel történhet. A látogatóknak a figyelmét fel kell hívni az érvényben lévő biztonsági előírásokra.

c) Az érzékeny területeken a jogosulatlan belépések kizárása, a belépések engedélyezése, figyelése, dokumentálása és ellenőrzése érdekében be- és kilépési naplót kell vezetni. A belépési naplót a rendszergazdák tárolják.

d) A szerverhelyiséget biztonsági ajtóval kell védeni.

e) Tilos a szerverhelyiség ajtaját nyitva hagyni, illetve tárggyal kiékelni.

f) Az érzékeny területek belépési naplóit, valamint a kiosztott jogosultságokat az IBF-nek évente ellenőriznie kell.

g) Az érzékeny területekre az ideiglenes jellegű munkát végző harmadik fél számára csak korlátozott mértékben és ellenőrzés mellett szabad biztosítani a hozzáférést. A felügyeletet a rendszergazda biztosítja.

h) A szerverszobában munkanapokon 18 órától 06 óráig, munkaszüneti napokon 0-24 óráig, illetve az utolsó rendszergazda távozása után elektronikus riasztórendszert kell alkalmazni.

i) A nyilvános helyen elhelyezett rack szekrényekben nyitásérzékelővel ellátott elektronikus riasztórendszert kell alkalmazni.

II.13.4. „Üres asztal - tiszta képernyő” politika

Az „üres asztal - tiszta képernyő” politika megvalósítása az alábbiakat jelenti:

a) A monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);

b) A felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;

c) A munkavégzés befejeztével a munkaállomásból ki kell jelentkezni, illetve ki kell azt kapcsolni;

d) Elfelejtés esetére jelszóvédett, automatikus zárolás kerül beállításra, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

e) A felhasználóknak az infokommunikációs eszközök elhelyezésére szolgáló helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik;

f) A kinyomtatott, faxolt vagy másolt iratokat nem szabad őrizetlenül a nyomtatókban, multifunkcionális eszközökben, fax-okban hagyni.

g) Ügyfelet és más külső felet nem szabad felügyelet nélkül az irodában hagyni.

II.13.5. A fizikai belépési engedélyek

El kell készíteni és napra készen kell tartani a Hivatalba belépésre jogosultak listáját. A belépésre jogosultak listája egyben a jogosultságot igazoló dokumentumként is szolgál. A belépésre jogosultak listáját a Hivatal elektronikus beléptető rendszere tárolja.

A listát a személyügyi referens fél évente dokumentáltan felülvizsgálja és törli a rendszerből a belépési jogosultsággal már nem rendelkező személyeket.

Amennyiben valakinek megszűnik a munkavégzésre irányuló jogviszonya, a személyügyi referensnek soron kívül törölnie kell az elektronikus beléptető rendszerből és vissza kell vennie a beléptető kártyáját.

A belépésre jogosultak listáját a Jegyző hagyja jóvá.

II.13.6. A fizikai belépés ellenőrzése

A fizikai belépéseket a jelen fejezetben foglaltak alapján kell megvalósítani.

II.13.6.1. Fizikai belépések

A Hivatal épületébe a belépés kizárólag a Hivatal főbejáratán lehetséges.

II.13.6.2. Fizikai belépések naplózása

A Hivatalba történő fizikai be- és kilépések tényét naplózni kell.

A Hivatalba történő be- és kilépéseket naplózni kell. A naplózást a jelenléti ívek vezetésével kell megvalósítani.

A jelenléti íveket 3 hónapig meg kell őrizni.

Ügyfélszolgálati időn kívül a Hivatal főbejárati ajtaját zárva kell tartani.

II.13.6.3. Kulcsok megóvása

Gondoskodni kell a védett munkaterületek ajtóinak kulcsainak megőrzéséről. Amennyiben a kulcsot a birtokosa elveszti, azonnal jelentenie kell a Jegyzőnek, aki gondoskodik az ajtó zárjának a cseréjéről.

II.13.6.4. Rendellenességek jelentése

Valamennyi Hivatali dolgozó kötelessége, hogy jelentse a jelen fejezetben leírt szabályokkal ellentétes viselkedést a Jegyzőnek, aki kivizsgálja az eseményt és dönt a szükséges további intézkedésekről.

II.13.7. Hozzáférés az érzékeny területekhez

Látogatók belépése az érzékeny területre csak hivatalos célból, ellenőrzötten és kísérővel történhet. A látogatóknak a figyelmét fel kell hívni az érvényben lévő biztonsági előírásokra.

Az érzékeny területeken a jogosulatlan belépések kizárása, a belépések engedélyezése, figyelése, dokumentálása és ellenőrzése érdekében belépési naplót kell vezetni.

A belépési naplót a Jegyzői titkárságon kell tárolni.

Az érzékeny területek elérésére a Jegyző, a rendszergazda és az IBF jogosultak. Minden más személy részére csak a Jegyző engedélyezheti a belépést az érzékeny területekre.

Az érzékeny területek belépési naplóit, valamint a kiosztott jogosultságokat az IBF-nek évente ellenőriznie kell.

Az érzékeny területekre az ideiglenes jellegű munkát végző harmadik fél számára csak korlátozott mértékben és ellenőrzés mellett szabad biztosítani a hozzáférést. A felügyeletet a rendszergazda biztosítja.

A szerverszobában munkanapokon 18 órától 06 óráig, munkaszüneti napokon 0-24 óráig, illetve az utolsó rendszergazda távozása után elektronikus riasztórendszert kell alkalmazni.

A nyilvános helyen elhelyezett rack szekrényekben nyitásérzékelővel ellátott elektronikus riasztórendszert kell alkalmazni.

II.13.8. Vendégek kísérete (*)

Biztosítani kell a Hivatalba érkező vendégek, ügyfelek kíséretét és regisztrációját, amennyiben védett munkaterületre lépnek be. A regisztrációt annak a munkatársnak kell elvégeznie, akihez a vendég érkezett. A regisztráció során rögzíteni kell a vendég nevét, a látogatás célját, az ügyintéző nevét, valamint a ki-és belépés időtartamát. A kíséretet annak a munkatársnak kell biztosítani, akihez a vendég érkezik.

II.13.9. A fizikai hozzáférések felügyelete (*)

A Hivatalnak ellenőriznie kell a fizikai hozzáféréseket az EIR-eket tartalmazó létesítményekben, hogy észlelje a fizikai biztonsági eseményeket és reagáljon rájuk.

Rendszeresen át kell vizsgálja a fizikai hozzáférések naplóit, és azonnal áttekinti azokat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak.

Össze kell hangolnia az ellenőrzések és vizsgálatok eredményeit a szervezet eseménykezelési képességével.

II.13.10. Látogatói hozzáférési naplók (*)

A látogatói naplókat 3 hónapig meg kell őrizni.

II.13.11. Vészvilágítás (*)

A Hivatalnak automatikus vészvilágítási rendszert kell működtetnie a létesítményben, amely áramszünet esetén aktiválódik, megvilágítja a vészkijáratokat és a menekülési útvonalakat.

II.13.12. Tűzvédelem (*)

A szerverhelyiségben független áramellátással ellátott tűzjelző készüléket, valamint elektromos tüzek oltására alkalmas tűzoltó készüléket kell alkalmazni.

A tűzvédelem részletszabályait a Hivatal Tűzvédelmi Szabályzata tartalmazza.

II.13.13. Környezeti védelmi intézkedések (*)

A szerverhelyiségben elhelyezett Hivatali kiszolgáló egységek biztonságos működése érdekében a hőmérsékletet 20-21 Celsius fok között kell tartani.

A hőmérsékletet az elhelyezett eszközök hő leadását figyelembe vevő, teljesítménnyel rendelkező klímaberendezéssel kell biztosítani.

A klímaberendezés által termelt kondenzvizet erre rendszeresített zárt csatornán ki kell vezetni a szerverhelyiségből.

A relatív páratartalom szintjét 40-60% között kell tartani.

A hőmérsékletet és a relatív páratartalom szintjét arra alkalmas eszközzel folyamatosan mérni kell. Az eszköznek riasztást kell adnia (pl.: SMS, email) a rendszergazdának, hogy ha a hőmérséklet 10 Celsius fok alá csökken vagy meghaladja a 28 Celsius fokot, illetve ha a relatív páratartalom szintje eléri a fent megadott határértéket.

II.13.14. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem (*)

Biztosítani kell, hogy víz- és más csővezetéken szállított anyag esetében a Jegyző által kijelölt személyek részére hozzáférhetőek legyenek a főelzáró szelepek.

a Jegyző felelőssége gondoskodni a főelzáró szelepek működőképességének fenntartásáról.

A szerverhelyiségben gondoskodni kell a víz és más csővezetékek kiváltásáról, vagy vízbetörés-érzékelő szonda felszereléséről.

II.13.15. Be- és kiszállítás

Szerviz részére eszközt csak a rendszergazda adhat át. Szervizbe történő szállítás esetén a szerviz által adott szállítólevelet a rendszergazda őrzi meg.

Szervizbe történő szállításkor vagy garanciális javítás esetén - jegyzőkönyv felvétele mellett – a rendszergazdának gondoskodnia kell az adatokat tartalmazó adathordozók törléséről vagy kiszereléséről.

A munkatársak részére hosszú távú használatra kiadott nagy értékű eszközökről (pl.: laptop) a Hivatalnak nyilvántartást kell vezetnie. Ezen eszközöket a munkatársak korlátozás nélkül ki- és beszállíthatják.

Minden más esetben eszközt kiszállítani csak a rendszergazdák írásos engedélyével lehet.

A ki- és beszállítások ellenőrzése a rendszergazda feladata. Infokommunikációs eszközök és berendezések írásos engedély nélküli ki- és beszállításának kísérlete esetét jelenteni kell az IBF-nek a szabálysértést elkövető személy felettes vezetőjének egyidejű értesítése mellett.

Az információbiztonsági tudatosság fokozását célzó oktatások keretében a felhasználókat tájékoztatni kell az ezzel kapcsolatos ellenőrzési feladatokról és jogokról.

II.14. TERVEZÉS

A technológiai vhr **TERVEZÉS** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.14.1. Szabályzat és eljárásrendek

A tudatossági és képzési eljárásrendet az IBSZ jelen fejezete tartalmazza.

II.14.2. Rendszerbiztonsági terv

El kell készíteni az elektronikus információs rendszerek rendszerbiztonsági tervét, mely a következőket tartalmazza:

a) az elektronikus információs rendszer hatóköre, alap feladatai (biztosítandó szolgáltatásait), biztonságkritikus elemei és alap funkciói;

b) az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztálya;

c) az elektronikus információs rendszer működési körülményei és más elektronikus információs rendszerrel való kapcsolatai.

Az elektronikus információs rendszer biztonsági követelményeit a vonatkozó rendszerdokumentációban kell rögzíteni.

Meg kell határozni a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedésbővítéseket, illetve végre kell hajtani a jogszabály szerinti biztonsági feladatokat.

Az elektronikus információs rendszerek rendszerbiztonsági tervét kétévente felül kell vizsgálni.

Soron kívül felül kell vizsgálni a rendszerbiztonsági terveket az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, illetve a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.

Az elektronikus információs rendszerek rendszerbiztonsági tervét az érintettek bevonásával a szállító készíti el.

A rendszerbiztonsági tervek bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, a Jegyző, valamint a Jegyző által írásban kijelölt személyek jogosultak.

II.14.3. Viselkedési szabályok

Az EIR-ek felhasználóira vonatkozó szabályokat a jelen IBSZ *{4. számú melléklet – Felhasználói Informatikai Biztonsági Házirend}* mellékletében foglalt Felhasználói Informatikai Biztonsági Házirend tartalmazza.

II.14.4. Viselkedési szabályok az interneten

A Hivatal által nyújtott internetkapcsolat és elektronikus levelezési szolgáltatás igénybevételének a következők a szabályai:

II.14.4.1. A web böngészés szabályai

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja! A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése), és adatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén az rendszergazda jelentést tesz az IBF-nek, aki eljár az ügyben a Jegyző felé.

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és Internet böngésző kontrollok is.

Tilos az IBF engedélye nélkül külső féllel nem web alapú hálózati kapcsolat kialakítása (pl.: FTP).

Tilos az elektronikus információs rendszerek használata a Hivatali értékekkel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes-, illetve szerencsejátékokra, bármilyen kereskedelmi, illetve jogellenes tevékenységre.

Tilos nem a munkavégzést szolgáló közösségi oldalak látogatása.

Tilos a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.

Főszabály szerint tilos Hivatali adatok felhő-alapú tárolása, illetve ezen adatok külföldi kezelése. Amennyiben felmerül a felhő-alapú és/vagy külföldi adatkezelés igénye, úgy a jelen IBSZ ***{Hiba! A hivatkozási forrás nem található.. Hiba! A hivatkozási forrás nem található.}*** jezetében foglaltak szerint kell eljárni.

Az internetről csak Hivatali célból lehet fájlokat letölteni! Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!

Az internetes oldalak elérése monitorozásra és naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

II.14.4.2. E-mail használat

A Hivatal által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag Hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos a Hivatali e-mail címüket nem Hivatali minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra, az Interneten elérhető nyilvános chat és fórum oldalakon Hivatali e-mail címmel hozzászólni stb.)!

A Hivatal által nem támogatott levelezőrendszer (pl.: G-mail, Freemail) használata munkavégzésre nem engedélyezett.

Az e-mail a munkavégzéssel kapcsolatos levelezést szolgálja, ahol az egy felhasználóra eső tárterület korlátozott és ennek túllépése esetén a rendszer figyelmeztetést küld, további figyelmeztetési határok átlépése esetén pedig megszűnhet a további levelezési lehetőség.

Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

A Hivatal elektronikus levelező rendszeréből elküldött elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására, mivel műszakilag - az elektronikus levelezési szolgáltatás működési elvéből fakadóan – a rendszergazdák nem tudnak garanciát vállalni arra, hogy az elektronikus levél

a) eljut a címzetthez;

b) átküldése közben illetéktelenek annak tartalmát el nem olvassák;

c) átküldése közben illetéktelenek annak tartalmát nem módosítják.

Amennyiben a fentiek biztosítására szükség van (pl.: elektronikus ügyintézés), akkor az állam által nyújtott Hivatali Elektronikus Ügyintézési Szolgáltatásokat kell igénybe venni, vagy egyéb kriptográfiai algoritmusokat kell alkalmazni az elküldött elektronikus levelek bizalmasságának és sértetlenségének biztosítása érdekében.

A fentiekhez hasonlóan a rendszergazdák arra sem tudnak garanciát vállalni, hogy egy Hivatali címzettnek szóló levél időben és sértetlenül megérkezik a címzetthez, mivel ehhez más, külső szolgáltatók közreműködése is szükséges, illetve a Hivatal a tömeges, kéretlen, valamint kártékony levelek elleni védekezésül spamszűrő rendszert működtet, mely kivételes esetben (fals pozitív) kiszűrhet hasznos levelet is.

A Hivatal elektronikus levelező rendszeréből csak akkor lehet bizalmas, jogszabály által védett adatot, titkot (személyes adatok, különleges adatok, adótitok stb.) elküldeni, hogy ha szabványos, sérülékenységektől mentes kriptográfiai algoritmussal az adat titkosításra került.

A felhasználók alapértelmezésben a levelezés során csak a saját postaládájukat tudják kezelni, mások postaládáit nem látják.

Más felhasználó postafiókjához történő hozzáférést az érintett postafiók felhasználója szervezeti egységének vezetője (az érintett felhasználó beleegyezésével) engedélyezi. Amennyiben a felhasználó beleegyezése nem szerezhető be (mert már megszűnt a jogviszonya, akkor is be kell tartani a hatályos adatvédelmi jogszabályok rendelkezéseit (fokozatosság elve, a részleteket a Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről című dokumentum tartalmazza).

A felhasználónak tilos a postafiókjában kezelt elektronikus levelek automatikus, vagy manuális továbbítása más, külső elektronikus levelező rendszerbe (pl.: a saját magán e-mail címére).

Zavaró, félreinformáló levelek, spamek küldése, jogtalan megrendelések elindítása tilos és eljárást vonhat maga után.

Ismeretlen helyről származó e-mailek, illetve azok csatolmányainak megnyitásakor és az azokban elhelyezett hivatkozásokra kattintással fokozott óvatossággal kell eljárni, mert maga az e-mail vagy annak csatolmánya, illetve az emailben elhelyezett hivatkozás kártékony lehet. Ebben az esetben ellenőrizni kell az e-mail feladóját, a tárgyat, a levél szövegezését (magyartalan megfogalmazás), a szükségtelen csatolmányokat és a levélben elhelyezett hivatkozásokat.

II.14.5. Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások

A Hivatal Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozásait a jelen IBSZ *{II.14.3. Viselkedési szabályok}* fejezete tartalmazza.

II.14.6. Biztonsági követelmények kiválasztása

A Hivatal a biztonsági osztályba sorolás során megállapított biztonsági osztályt alapul véve állapítja meg az EIR biztonsági követelményeit.

II.14.7. Biztonsági követelmények testre szabása

A Hivatal jelen IBSZ-ben foglaltak alapján valósítja meg az EIR-ek biztonsági követelményeit.

II.15. SZEMÉLYI BIZTONSÁG

A technológiai vhr **SZEMÉLYI BIZTONSÁG** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.15.1. Szabályzat és eljárásrendek

A személyi biztonsági eljárásrendet az IBSZ jelen fejezete tartalmazza.

II.15.2. Munkakörök biztonsági szempontú besorolása (*)

A Hivatal az információbiztonsági szempontból alap és kiemelt munkaköröket állapított meg.

A Hivatalnál nincsenek nemzetbiztonsági ellenőrzés alá eső munkakörök és feladatok.

II.15.2.1. Alap biztonsági osztály

Az alap biztonsági osztályba a következő munkakörök kerültek besorolásra:

a) Adatgazda,

b) Felhasználó.

Az alap munkakör betöltésének követelményei:

a) Erkölcsi bizonyítvány,

b) Szakirányú végzettség,

c) Informatikai alapismeretek,

II.15.2.2. Kiemelt biztonsági osztály

A kiemelt biztonsági osztályba a következő munkakörök tartoznak:

a) Jegyző, és jegyzőhelyettesek

b) Rendszergazda,

c) Információbiztonsági felelős.

A kiemelt biztonsági munkakör betöltésének követelményei:

a) Erkölcsi bizonyítvány

b) Szakirányú végzettség

c) 2 év szakmai tapasztalat

II.15.3. Személyek háttérellenőrzése (*)

Az Hivatal személyügyi referensének a feladata, hogy az elektronikus információs rendszerekhez való hozzáférési jogosultság megadása előtt ellenőrizze, hogy az érintett személy a *{II.15.2 Munkakörök biztonsági szempontú besorolása (*)}* fejezetben meghatározott feltételeknek megfelel-e. A vizsgálat magában foglalja az alábbiakat:

a) referenciák ellenőrzése,

b) a felvételre jelentkező életrajzának ellenőrzése a teljességre és pontosságra vonatkozóan,

c) a legmagasabb iskolai végzettség (szakképzettség) ellenőrzése,

d) nyelvtudást igazoló okiratok ellenőrzése,

e) hatóság által kibocsátott azonosító irat ellenőrzése,

f) erkölcsi bizonyítvány ellenőrzése.

Külső szerződő felek esetében a szerződést kezdeményező feladata a szerződésben előírni a személybiztonsági feltételeket.

II.15.4. Személyek munkaviszonyának megszűnése

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges:

a) Jogosultságok dokumentált formában történő megszüntetése.

b) A felhasználó elektronikusan tárolt információit, e-mailjeit és egyéb általa létrehozott adatot menteni, archiválni kell az általa használt informatikai eszközről, szerver tárhelyről, illetve bármely egyéb adathordozóról.

c) Az így archivált adatokat a törvényi előírásoknak megfelelően tárolni kell, illetve 1 év után törölni kell a rendszerből.

A fentiek végrehajtását a jogviszony megszűnésével egy időben, kockázatot jelentő esetekben a jogviszony megszűnését megelőzőn kell végrehajtani. A végrehajtás elrendeléséért a Jegyző, a végrehajtásért a rendszergazda a felelős.

Kiemelt biztonsági osztályba tartozó munkakörök esetén a jogviszony megszűntetését információbiztonsági szempontból az IBF koordinálja.

Az érintett felhasználó elektronikus levelezést tartalmazó postafiókjának áttekintése során kell be kell tartani a hatályos adatvédelmi jogszabályok rendelkezéseit (fokozatosság elve, a részleteket a Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről című dokumentum tartalmazza).

II.15.4.1. Vagyontárgyak visszaszolgáltatása

Valamennyi felhasználónak, a szerződőknek és a felhasználó harmadik félnek vissza kell szolgáltatnia az Hivatal valamennyi használatra átvett vagyontárgyát, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik.

A rendszergazdának az eszköz leadásakor ellenőriznie kell, hogy a felhasználó az átvételi elismervényben rögzített hardver-, szoftver specifikációval adja-e vissza a vagyontárgyat.

II.15.4.2. Hozzáférési jogok megszüntetése

Valamennyi alkalmazottnak, a szerződőknek és a felhasználó harmadik feleknek információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár.

A fentiektől eltérni a Jegyző írásos engedélyével lehetséges.

A feladatok végrehajtásáért a rendszergazda a felelős.

II.15.4.3. Információbiztonsági kötelmek a jogviszony megszűnése után

A személyügyi referensnek a jelen IBSZ *{7. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén}* mellékletében foglaltak szerint tájékoztatnia kell a dolgozót arról, hogy

a) legkésőbb a jogviszony megszűnése napján köteles az Hivatal elektronikus információs rendszerével kapcsolatos valamennyi eszközt hiánytalanul, sértetlenül munkáltatója részére visszaszolgáltatni;

b) a Hivatalnál működő elektronikus információs rendszereket az Hivatal kizárólag Hivatali munkavégzés céljából biztosítja a munkatársak részére, az elektronikus információs rendszerekben keletkező és ott tárolt, kezelt adatok, információk vonatkozásában a Hivatal fenntartja magának a tulajdonjogot;

c) a Hivatalnak továbbra is hozzáférési lehetősége van az általa korábban használt, kezelt elektronikus információs rendszerekhez és az azokban kezelt adatokhoz;

d) a titoktartási kötelezettsége a jogviszonya megszűnését követően is fennáll.

A fentiek megsértése jogi következményeket von maga után.

II.15.5. Az áthelyezések, átirányítások és kirendelések kezelése

Az áthelyezés során el kell végezni az érintett munkatárs ellenőrzését a jelen IBSZ *{II.15.3. Személyek háttérellenőrzése (*)}* pontjában foglaltak alapján.

Az érintett munkatárs részére az elektronikus információs rendszerhez történő logikai és fizikai hozzáférések engedélyezését a jelen IBSZ *{II.3.4. Hozzáférési jogok igénylésének eljárásrendje}* pontjában foglaltaknak megfelelően kell elvégezni.

Szükség esetén el kell végezni az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését.

A jogviszony megváltozásáról a Jegyző értesíti a munkatárs régi, valamint új vezetőjét.

II.15.6. Hozzáférési megállapodások (*)

A hozzáférési megállapodásokra vonatkozó követelményeket a jelen IBSZ *{II.17.5. Harmadik felekkel kapcsolatos előírások}* fejezete tartalmazza.

II.15.7. Külső személyekhez kapcsolódó biztonsági követelmények (*)

A harmadik féllel kötött szerződésekben - amennyiben az értelmezhető - az alábbiakat kell előírni:

a) A külső szervezetnek meg kell határoznia az Hivatallal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat;

b) Meg kell követelni, hogy a szerződő fél feleljen meg a Hivatal által meghatározott személybiztonsági követelményeknek;

c) Meg kell követelni, hogy a szerződő fél dokumentálja a személybiztonsági követelményeket;

d) Elő kell írni, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az Hivatal elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az Hivatalnak;

e) Az informatikai biztonság fő szabályait;

f) Az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának meghatározását, illetve a védelem érdekében meghatározott eljárásokat;

g) Az információk másolásának és nyilvánosságra hozatalának feltételeit;

h) A szolgáltatás elvárt szintjének és a szolgáltatási időszaknak a meghatározását;

i) A felek felelősségének meghatározását;

j) A szellemi tulajdon védelmére és másolására vonatkozó jogokat és kötelezettségeket;

k) A teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését;

l) A felmerülő problémák kezelését;

m) A hardver- és szoftvertelepítésből és karbantartásokból eredő felelősséget;

n) Világos és egyértelmű jelentéskészítési struktúrát és rendszert;

o) A változáskezelések egyértelmű és meghatározott folyamatát;

p) Óvintézkedések meghatározását a kártékony kódok ellen;

q) Biztonsági események kivizsgálására és jelentésére vonatkozó intézkedések meghatározását;

r) Az alvállalkozók bevonására vonatkozó szabályokat.

Abban az esetben, ha a feladat elvégzésére a harmadik fél alvállalkozót is igénybe vesz, a szerződésben pontosan meg kell nevezni az alvállalkozót, s meg kell határozni a rá vonatkozó hozzáférési jogosultságokat. A titoktartási kötelezettség a harmadik fél alvállalkozójára is vonatkozik, és a szerződésnek titoktartási nyilatkozat részt is kell tartalmaznia.

II.15.8. Fegyelmi intézkedések

A jelen IBSZ-ben előírt szabályok megszegéséről az észlelő haladéktalanul köteles tájékoztatni az IBF-et. Az IBF a tudomására jutott események súlyosságát mérlegeli, és szükség esetén jelenti a Jegyzőnek.

A biztonsági előírások megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor, amelyet az IBF által felterjesztett jelentés alapján a Jegyző kezdeményez. Az eljárás a jogszabályok és a Hivatal belső szabályai szerint történik.

Külső szerződő fél által elkövetett szabályszegés esetében a szerződésben foglaltak szerint, illetve a vonatkozó jogszabályok alapján kell eljárni.

II.15.9. Munkaköri leírások (*)

A Hivatalnak rögzítenie kell a jelen IBSZ *{II.15.2. Munkakörök biztonsági szempontú besorolása (*)}* foglalt biztonsági szerepköröket és felelősségeket a szervezeti munkaköri leírásokba.

II.16. KOCKÁZATKEZELÉS

A technológiai vhr **KOCKÁZATKEZELÉS** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.16.1. Adatosztályozás

Annak érdekében, hogy a Hivatal által kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszerben kezelt adatok bizalmasság, sértetlenség és rendelkezésre állás szerinti osztályozására a Kiber vhr.3.§-ában foglaltak szerint.

Az adatosztályozást nem privát felhőszolgáltatás igénybevétele és külföldi adatkezelés megvalósítása esetén köteles elvégezni, a külföldi vagy nem privát felhőszolgáltatás igénybevételével történő adatkezelés kockázatainak felmérése érdekében.

Az adatosztályozás során figyelembe kell venni a logikailag együtt, egységben kezelt elektronikus adatok – ideértve az adatbázist, adattárat, egyedi dokumentumot és egyéb adatállományt – együttes biztonsági igényét.

A Hivatal az adatosztályozás alapján, annak eredményére tekintettel vehet igénybe nem privát felhőszolgáltatást, vagy kezelhet külföldön adatot, amennyiben más jogszabály a felhőszolgáltatás igénybevételét, vagy a külföldi adatkezelést nem tiltja vagy korlátozza.

A Hivatal a biztonsági osztályba sorolás keretében, valamint abban az esetben vizsgálja felül az adatosztályozást, amennyiben az elektronikus információs rendszerben kezelendő adatok körében változás következik be.

II.16.2. Biztonsági osztályba sorolás

A Hivatalnak az Kibertv. 6. § (10) b) bekezdése alapján nem kell biztonsági osztályba sorolnia az elektronikus információs rendszereit.

II.16.3. Kockázatelemzés

A kockázatelemzést a jelen IBSZ *{3.* számú melléklet – Kockázatelemzési és kezelési módszertan*}* mellékletében leírt módszertan alapján az IBF végzi el.

A kockázatelemzést évente el kell végezni, melynek során felül kell vizsgálni az előző évi kockázatelemzés eredményét. A kockázatelemzést soron kívül el kell végezni, hogy ha

a) változás áll be az elektronikus információs rendszerben, vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését),

b) olyan körülmények következnek be, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát.

A kockázatelemzés eredményét IBF-nek dokumentálnia kell, majd meg kell ismertetnie a Jegyzővel.

A nem tolerálható kockázatok kezelésére intézkedési tervet kell készíteni, melynek tartalmaznia kell a kockázat kezelésére javasolt intézkedéseket, felelős, határidő és költségvonzat megjelölésével.

A kockázatkezelési tervet az IBF-nek kell előkészítenie és a Jegyző hagyja jóvá.

A kockázatelemzéssel és kezeléssel kapcsolatos dokumentumok bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, a Jegyző, valamint a Jegyző által írásban kijelölt személyek jogosultak.

II.16.4. Kockázatelemzés – Ellátási lánc (*)

A Hivatalnak fel kell mérnie az ellátási lánc kockázatait a meghatározott EIR-jei, rendszerelemei és rendszerszolgáltatásai vonatkozásában.

Meghatározott időközönként frissíti az ellátási lánc kockázatelemzését, amikor jelentős változások történnek az érintett ellátási láncban, vagy amikor a rendszer, a működési környezet vagy más körülmények változása esetén szükségessé válhat az ellátási lánc megváltoztatása.

II.16.5. Sérülékenységek ellenőrzése (*)

A Hivatalnak évente ellenőriznie kell az EIR sérülékenységeit, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek.

A feltárt sérülékenységeket javítani kell a kockázatkezelési eljárásoknak megfelelően.

II.16.6. Sérülékenységmenedzsment – Sérülékenységi információk fogadása (*)

A szervezet létrehoz egy csatornát, amelyen keresztül fogadhatja a szervezeti EIR-ekben és rendszerelemekben található sérülékenységekről szóló jelentéseket.

II.16.7. Kockázatokra adott válasz (*)

A szervezet a kockázatmenedzsment szabályokkal összhangban reagál a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításaira.

II.17. RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS

A technológiai vhr **RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.17.1. Szabályzat és eljárásrendek

Az Hivatal rendszer- és szolgáltatásbeszerzésre vonatkozó szabályzatát az IBSZ jelen fejezete tartalmazza.

II.17.2. Erőforrások rendelkezésre állása (*)

Az éves költségvetési tervezési folyamatban ki kell térni az elektronikus információs rendszerek biztonsági beruházásainak tervezésére, oly módon, hogy a Hivatal költségvetésében elkülönítetten szerepeljen.

A biztonsági beruházások tervezését az informatikai biztonsági stratégiai célok, valamint a cselekvési tervekben megfogalmazottak alapján kell elkészíteni.

A tervezési dokumentumot az információbiztonsági felelős készíti el az informatikai területért felelős vezetővel együttműködve.

A tervezési dokumentumban legalább a következőket kell feltüntetni:

a) beruházás megnevezése;

b) beruházás indoka, célja, kezelt kockázat;

c) költség-hasznon elemzés;

d) a beruházás elhagyásának következményei (jogi, információbiztonsági kockázat).

Az információbiztonsági beruházások tervezését tartalmazó előterjesztést – az informatikai beruházások tervezésével együtt - az informatikai területért felelős vezető terjeszti be a Jegyző részére jóváhagyás céljából.

II.17.3. A rendszer fejlesztési életciklusa (*)

Az elektronikus információs rendszerek életciklusait a következő fejezetben leírtak szerint kell meghatározni:

II.17.3.1. Követelmény meghatározás

A beszerzés előtt dokumentált formában, részletesen meg kell határozni a felhasználói és az információbiztonsági követelményeket a jelen IBSZ *{II.17.4. Beszerzések (*)}* fejezetében meghatározottak alapján.

A felhasználói követelményeket az adatgazdának, az információbiztonsági követelményeket az IBF-nek kell meghatároznia.

II.17.3.2. Fejlesztés/beszerzés

A fejlesztés/beszerzés fázisában az IBF-nek folyamatosan képviselni kell az IBSZ-ben, illetve az információbiztonsági követelményekben foglaltak teljesülését a jelen IBSZ *{II.17.4. Beszerzések (*)}* fejezetében meghatározottak alapján.

II.17.3.3. Megvalósítás/értékelés

Az éles bevezetés előtt tesztkörnyezetben funkcionális, biztonsági és üzemeltetési teszteket kell folytatni. A tesztek a rendszerdokumentációkban megfogalmazott elvárások bizonyítására szolgálnak.

A bevezetésről a Jegyző dönt az adatgazda, az Üzemeltetési Osztály vezetője és az IBF javaslatára.

A jelen fejezetben foglaltakra a jelen IBSZ *{II.17.4.* Beszerzések (*)*}* fejezetében meghatározottak az irányadók.

II.17.3.4. Üzemeltetés és fenntartás

Az üzemeltetés és fenntartás során valamennyi érintett félnek be kell tartania az IBSZ-ben foglalt követelményeket.

II.17.3.5. Kivonás (archiválás, megsemmisítés).

Elektronikus információs rendszer kivonása esetén értesíteni kell a Hatóságot az érintett EIR kivonásáról, valamint felül kell vizsgálni az IBSZ-t.

Kivonáskor az EIR-ben tárolt adatok archiválása után (figyelemmel az adatvédelmi előírásokra) az adathordozók újrafelhasználása vagy selejtezése esetében, a jelen IBSZ *{II.12.4. Az infokommunikációs eszközök biztonságos újrahasznosítása, mások rendelkezésére bocsátása, selejtezése}* pontjában leírtak, illetve az Hivatal Selejtezési Szabályzata az irányadó.

II.17.4. Beszerzések (*)

A Hivatal informatikai tárgyú beszerzései során a következő eljárásrendet kell követni.

II.17.4.1. Funkcionális biztonsági követelmények

A kockázatokkal arányos védelem kialakítása érdekében az IBF-et még a tervezés (ajánlatkérés) fázis elejétől kezdve be kell vonni a projektbe.

Az IBF bevonása a szerződést kezdeményező szervezeti egység vezetőjének feladata és felelőssége.

A tervezés fázisában az adatgazdának az IBF-fel együttműködve biztonsági osztályba kell sorolni az alkalmazni kívánt EIR-t.

Az IBF-nek a megállapított biztonsági osztály alapján meg kell határoznia a szállító felé a vonatkozó adminisztratív, fizikai és logikai védelmi intézkedéseket.

Webes alkalmazás fejlesztés esetén elő kell írni, hogy a fejlesztés feleljen meg az *{Open Web Application Security Project Application Security Verification Standard (ASVS) aktuális verziója}* –ban rögzített, IBF által meghatározott követelményeknek.

Mobil alkalmazás fejlesztése során elő kell írni, hogy a fejlesztés feleljen meg *{Open Web Application Security Project Mobile Application Security Verification Standard aktuális verziója}*-ban rögzített, IBF által meghatározott követelményeknek.

A szállító által teljesítendő védelmi intézkedéseket a szerződés mellékletévé kell tenni. A szállítónak dokumentált módon el kell készítenie a fentiekben meghatározott védelmi intézkedések alapján a szállítandó termék funkcionális biztonsági követelményeit, azaz ki kell fejtenie, hogy az adott követelményt konkrétan hogyan, milyen módon fogja teljesíteni az általa szállítandó rendszer vonatkozásában.

Az IBF-fel a tervezés fázisában el kell fogadtatni a funkcionális biztonsági követelményeket, anélkül az EIR fejlesztése nem kezdhető meg.

II.17.4.2. Garanciális biztonsági követelmények

A biztonsági intézkedések fejtsék ki hatásukat, és teljesítsék a bennük közvetlenül megfogalmazott funkcionális követelményeket. A szállítóknak el kell készíteniük az intézkedések funkcionális leírását és tervét olyan részletességgel, amely lehetővé teszi az intézkedések elemzését és tesztelését (ideértve az intézkedést megvalósító összetevők közötti funkcionális interfészeket is). A szállítók az intézkedések szerves részeként szerepeltessék a kiosztott felelősségeket és speciális tevékenységeket annak érdekében, hogy amikor az intézkedéseket megvalósítják, azok folyamatosan és következetesen (azaz az informatikai célrendszer egészében) teljesítsék megkívánt feladatukat vagy céljukat, továbbá segítsék az intézkedések hatékonyságának javítását.

Az intézkedéseket oly módon dolgozzák ki, hogy nagy biztonsággal támogatni tudják azt, hogy az intézkedések összessége teljes, konzisztens és helyes.

II.17.4.3. Az elektronikus információs rendszer fejlesztési környezetére vonatkozó előírások

A szerződésekben elő kell írni, hogy a leszállított szoftver megfelelően biztonságos környezetben, auditálható körülmények között készüljön. A leszállított szoftver nem tartalmazhat a dokumentációkban nem rögzített szükségtelen funkcionalitást, nem tartalmazhat hátsó kaput, illetve egyéb kártékony kódot. Amennyiben mégis tartalmazna, és ebből adódóan a Hivatalnak bármilyen kára keletkezne, akkor azért a Szállító felelősséggel tartozik.

A Hivatal részére történő fejlesztések során csak olyan szoftverkomponensek használhatóak fel, melyek nemzetközileg széles körben elfogadottak, rendelkeznek megfelelő gyártói támogatással a felfedezett biztonsági rések javítására és a gyártói támogatásuk még legalább 3 évig érvényes.

II.17.4.4. Az elektronikus információs rendszer tervezett üzemeltetési környezetére vonatkozó előírások

Amennyiben az elektronikus információs rendszert a Hivatal fogja üzemeltetni, a tervezés fázisában egyeztetni kell a rendszergazdákkal az általuk támogatható futtatókörnyezetet és annak erőforrásigényét (hardverigény, licencek száma stb.). A rendszerdokumentációkban rögzíteni kell a tervezett futtatókörnyezet leírását.

II.17.5. Harmadik felekkel kapcsolatos előírások

Harmadik fél csak egyedi esetben, meghatározott időre és meghatározott feladat ellátásához látható el jogosultsággal, amit szerződésben kell dokumentálni. A hozzáférést az elektronikus információs rendszer adatgazdájának kell engedélyezni.

A Hivatal és szerződéses partnerei szerződésben rögzített, a jelen IBSZ-nek megfelelő biztonsági intézkedéseket kötelesek foganatosítani annak érdekében, hogy a kicserélt (átadott/átvett) adatok és dokumentumok véletlen vagy szándékos kompromittálódását megakadályozzák.

A harmadik félnek a Hivatal elektronikus információs rendszereihez történő hozzáférése esetében - figyelembe véve a szükséges hozzáférési típusokat, az információ értékét, a harmadik fél által alkalmazott biztosítékokat, valamint a hozzáférés mélységét - törekedni kell a kockázatok minimalizálására.

Azokban az esetekben, amelyekben az információ feldolgozása vagy kezelése kiszervezéssel történik, a harmadik féllel kötött szerződésnek a betartandó biztonsági követelményeket is tartalmaznia kell.

Harmadik fél hozzáférését a Hivatal adataihoz és információihoz, a munkájához elengedhetetlenül szükséges minimum szintre kell korlátozni. A hozzáférések feltételeit szerződésben kell részletezni. A szerződés csak a Hivatal jelen IBSZ-ével összhangban lévő követelményeket tartalmazhat.

A szerződésnek tartalmaznia kell továbbá a bizalmasságra, a szellemi tulajdonjogokra, a szerzői jogok átruházására és minden közösen végzett munkálatok védelmére vonatkozó nem nyilvános garanciákat is.

A szerződésben elő kell írni, hogy a Hivatal információs vagyonelemei a szerződés lejártát követően kerüljenek vissza a Hivatal birtokába, a szerződött félnél - valamint annak partnereinél, alvállalkozóinál - pedig kerüljenek megsemmisítésre.

A szerződéses partnernek a Hivatallal egyeztetnie kell a számára nyújtott szolgáltatásokkal kapcsolatos minden részdöntést.

A szerződésben a Hivatal számára jogot kell biztosítani arra, hogy a már kölcsönösen elfogadott szerződéses felelősséget felülvizsgálja, szükség esetén harmadik féllel felülvizsgáltassa.

Harmadik fél a Hivatal adatait és az elektronikus információs rendszereit a hozzáférést rögzítő szerződés és a jelen IBSZ *{8. számú melléklet – Titoktartási Nyilatkozat}* mellékletében található titoktartási nyilatkozat aláírása előtt nem ismerheti meg.

II.17.5.1. A harmadik fél hozzáférési kockázatának azonosítása

A Hivatalnak fel kell mérnie, és meg kell határoznia, hogy mekkora a kockázata annak, ha a harmadik félnek hozzáférési joga van a Hivatal információs vagyonához.

A kockázatok felmérése a jelen IBSZ *{2. számú melléklet – Kockázatelemzési és kezelési módszertan}* melléklete szerint történik. A kockázatkezeléshez, a megfelelő óvintézkedések kialakításához és a hozzáférések engedélyezéséhez a hozzáférés igénylésben pontosan meg kell határozni a hozzáférések típusát és azt, hogy milyen okból történik a hozzáférés.

A kockázat meghatározásért a harmadik féllel kötött szerződés teljesítésében elsődlegesen érintett szervezeti egység vezetője a felelős, és a szerződés megkötése előtt köteles az informatikai biztonsági felelőst bevonni a szerződéskészítés folyamatába.

II.17.5.2. A harmadik féllel kötött szerződés biztonsági követelményei

A szerződésekben, amennyiben az értelmezhető az alábbiakat kell előírni:

a) a külső szervezetnek meg kell határoznia a Hivatallal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat;

b) meg kell követelni, hogy a szerződő fél feleljen meg a Hivatal által meghatározott személybiztonsági követelményeknek;

c) meg kell követelni, hogy a szerződő fél dokumentálja a személybiztonsági követelményeket;

d) elő kell írni, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Törvényszék elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést a Hivatalnak;

e) az informatikai biztonság fő szabályait;

f) az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának meghatározását, illetve a védelem érdekében meghatározott eljárásokat;

g) az információk másolásának és nyilvánosságra hozatalának feltételeit;

h) a szolgáltatás elvárt szintjének és a szolgáltatási időszaknak a meghatározását;

i) a felek felelősségének meghatározását;

j) a szellemi tulajdon védelmére és másolására vonatkozó jogokat és kötelezettségeket;

k) a teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését;

l) a felmerülő problémák kezelését;

m) a hardver- és szoftvertelepítésből és karbantartásokból eredő felelősséget;

n) világos és egyértelmű jelentéskészítési struktúrát és rendszert;

o) a változáskezelések egyértelmű és meghatározott folyamatát;

p) óvintézkedések meghatározását a kártékony kódok ellen;

q) biztonsági események kivizsgálására és jelentésére vonatkozó intézkedések meghatározását;

r) az alvállalkozók bevonására vonatkozó szabályokat.

Abban az esetben, ha a feladat elvégzésére a harmadik fél alvállalkozót is igénybe vesz, a szerződésben pontosan meg kell nevezni az alvállalkozót, s meg kell határozni a rá vonatkozó hozzáférési jogosultságokat. A titoktartási kötelezettség a harmadik fél alvállalkozójára is vonatkozik, és a szerződésnek titoktartási nyilatkozat részt is kell tartalmaznia.

II.17.5.3. Fejlesztési szerződések biztonsági követelményei

A fejlesztést végző külső féllel megkötendő szerződésnek a következőket kell tartalmaznia:

Minden egyes, a Hivatal elektronikus információs rendszerével kapcsolatba kerülő fejlesztési vagy bővítési projektnél figyelembe kell venni a Hivatal érvényben lévő, vonatkozó szabályzatait, különös tekintettel az IBSZ-re, annak tudomásul vételét és elfogadását a szerződésben rögzíteni kell.

Elő kell írni a jelen IBSZ *{II.17.5.3 Fejlesztési szerződések biztonsági követelményei}* fejezetében megkövetelt biztonsági dokumentációk elkészítését.

A szerződésben meg kell követelni, hogy a fejlesztő, szállító hozza létre és bocsássa rendelkezésére jelen IBSZ *{II.17.4.1. Funkcionális biztonsági követelmények}* fejezetében megkövetelt, az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

A szerződésben elő kell írni, hogy minden egyes új verzióra kiterjedően a szoftver forráskódját és fordítási paramétereit át kell adni a Hivatal részére, vagy azokat letétbe kell helyezni arra kijelölt harmadik személynél olyan formában, hogy a támogató cég megszűnése esetén a kód a Hivatal számára hozzáférhető legyen. A szerződésben rögzíteni kell az érintett EIR tovább használhatóságának a feltételeit abban az esetben, hogy ha a támogató cég szerződése megszűnik a Hivatallal.

II.17.5.4. Támogatási szerződések

Az elektronikus információs rendszerek támogatási szerződéseiben a következőket kell előírni:

a) az EIR-ben felmerülő hibák kezelése, javítása,

b) a Hivatal fejlesztési igényeinek ellátása,

c) megállapodás alapján az EIR futtató környezetének (operációs rendszer, adatbázis rendszerek, egyéb szoftverkomponensek) frissítése.

A szerződésben rögzíteni kell a támogatás körülményeit (határidők, rendelkezésre állás, helyszíni vagy telefonos támogatás) is a megfelelő szolgáltatási szint biztosítására. A paraméterek pontos értékének meghatározása az EIR adatgazdájának a feladata.

II.17.6. Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai (*)

A Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságaira vonatkozó követelményeket a jelen IBSZ *{II.17.6. Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai}* fejezete tartalmazza.

II.17.7. Az elektronikus információs rendszerre vonatkozó dokumentáció

A szállítónak - szükség szerint az IBF-fel és a rendszergazdákkal együttműködve - a következő dokumentumokat kell elkészítenie az átadás-átvétel előtt:

a) az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját, amely tartalmazza:

   aa) az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését;

   ab) a biztonsági funkciók hatékony használatát és karbantartását; valamint

   ac) az ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban.

b) a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját, amely tartalmazza:

   aa) a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját;

   ab) a felhasználói interakció biztonságos módját;

ac) a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában

c) Rendszerbiztonsági terv, mely tartalmazza a szállítandó termék/fejlesztés biztonsági intézkedéseinek funkcionális biztonsági leírását.

Amennyiben nem áll rendelkezésre vagy nem létezik adminisztrátori, üzemeltetői és felhasználói dokumentáció, úgy a szervezet dokumentálja az EIR, rendszerelem vagy rendszerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, és a dokumentációkat eljuttatja a szervezet által meghatározott személyeknek vagy szerepköröknek.

Egyedi fejlesztések esetében a következő, további dokumentumokat kell a szállítónak elkészítenie és átadnia:

a) követelményspecifikáció;

b) rendszerterv;

c) teszteseteket tartalmazó tesztelési forgatókönyv.

II.17.7.1. Dokumentálás formai követelményei

Az EIR dokumentálása során az alábbi pontokban részletezett formai elemeket minden dokumentumban értelemszerűen kell szerepeltetni.

a) Dokumentum adatlap:

aa) a dokumentum címe,

ab) tárgya,

ac) fájl neve és verziója,

ad) dokumentum típusa,

ae) dokumentum verziószáma,

af) dokumentum státusza,

ag) dátum,

ah) Készítő, Ellenőr,

ai) verziószám,

aj) státusz,

ak) minősítés.

b) lapszámozás,

c) tartalomjegyzék,

d) tárgymutató.

II.17.7.2. Dokumentumok rendelkezésre állása

Az EIR dokumentációjának egy eredeti nyomtatott példányban és szerkeszthető Open Document Format (ODF)-ban, vagy Microsoft Word formátumban és nyomtatható PDF formátumban, elektronikus formában kell rendelkezésre állnia.

II.17.7.3. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények

Gondoskodni kell a biztonsággal kapcsolatos dokumentumok illetéktelenek elleni védelméről az EIR teljes életciklusa (létrehozás, módosítás, megsemmisítés) alatt.

A biztonsággal kapcsolatos dokumentumokat a következő szerepkörök ismerhetik meg:

a) fejlesztő;

b) rendszergazda;

c) IBF;

d) Jegyző.

II.17.8. Biztonságtervezési elvek

A Hivatal biztonságtervezési elveit az IBSZ jelen fejezetei tartalmazzák.

II.17.9. Külső elektronikus információs rendszerek szolgáltatásai

Külső elektronikus információs rendszerek igénybevétele esetén a jelen IBSZ *{II.17.5.3. Fejlesztési szerződések biztonsági követelményei}* pontjában foglaltakon kívül szerződésben kell rögzíteni az érintett EIR biztonsági osztályát és a szolgáltató által teljesítendő, az érintett EIR biztonsági osztályából fakadó adminisztratív, fizikai és logikai védelmi intézkedéseket.

A szerződésben ki kell térni a Hivatal felhasználóinak feladataira az igénybe vett külső elektronikus információs rendszerek szolgáltatásával kapcsolatban.

A szerződésben ki kell kötni a jogot arra, hogy a Hivatal az IBF útján auditálhassa a szolgáltatónál kialakított, szerződésben meghatározott védelmi intézkedéseket.

II.17.10. Támogatással nem rendelkező rendszerelemek (*)

A Hivatalnak le kell cserélnie a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól.

A Hivatalnak a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást kell biztosítania, amelyet belső erőforrásokkal, vagy a szervezet által meghatározott külső szolgáltatók bevonásával valósít meg.

II.18. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

A technológiai vhr **RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.18.1. Szabályzat és eljárásrendek

A Hivatal rendszer- és kommunikációvédelmi eljárásrendjét az IBSZ jelen fejezete tartalmazza.

II.18.2. Szolgáltatásmegtagadással járó támadások elleni védelem (*)

A Hivatal elektronikus információs rendszereit hálózati, infrastruktúra és alkalmazás szinten is fel kell készíteni a szolgáltatás megtagadás alapú támadásokkal szemben.

II.18.2.1. Hálózati szint

Hálózati szinten a következőket kell végrehajtani a túlterhelés elleni védelem megvalósítása érdekében:

a) A határvédelmi rendszert a jelen IBSZ *{II.18.3A határok védelme}* fejezetében leírtak alapján kell konfigurálni;

b) Különös figyelmet kell fordítani a menedzsment portok kommunikációjának titkosítására, elérhetőségének korlátozására (pl.: IP cím szűrés).

c) Biztosítani kell a hálózati eszközöket alkotó szoftverkomponensek naprakészségét a jelen IBSZ *{II.19.2. Hibajavítás}* fejezetében leírtak szerint.

d) Az érintett hálózati eszközöket úgy kell konfigurálni, hogy csak a minimálisan szükséges portok, protokollok és szolgáltatások legyenek engedélyezve.

e) Hálózati szinten a Hivatal határvédelmi rendszerében és a Hivatali Wi-Fi kontrollerében be kell kapcsolni a túlterhelés - szolgáltatás megtagadás alapú támadás – elleni védelmet.

II.18.2.2. Infrastruktúra szint

Infrastruktúra szintjén a következőket kell végrehajtani a túlterhelés elleni védelem megvalósítása érdekében:

a) Biztosítani kell az érintett rendszert alkotó szoftverkomponensek naprakészségét a jelen IBSZ *{II.19.2. Hibajavítás}* fejezetében leírtak szerint;

b) Az érintett rendszert infrastruktúra úgy kell konfigurálni, hogy csak a minimálisan szükséges portok, protokollok és szolgáltatások legyenek engedélyezve;

c) Az érintett rendszer kártékony kód elleni védelmét a jelen IBSZ *{II.19.3. Kártékony kódok elleni védelem}.* fejezetében leírtak szerint kell megvalósítani.

II.18.2.3. Alkalmazás szint

Alkalmazás szinten a következőket kell végrehajtani a túlterhelés elleni védelem megvalósítása érdekében:

a) Biztosítani kell alkalmazás szinten az érintett rendszert alkotó szoftverkomponensek naprakészségét a jelen IBSZ *{II.19.2. Hibajavítás}* fejezetében leírtak szerint.

b) Az érintett rendszert alkalmazás szinten úgy kell konfigurálni, hogy csak a minimálisan szükséges portok, protokollok és szolgáltatások legyenek engedélyezve.

c) Alkalmazás szinten különböző csillapítási technikákat kell alkalmazni (pl.: Captcha kód, meghatározott küszöbszámok elérésre után forrás IP cím korlátozása stb.) a felhasználó felületeket érő szolgáltatás megtagadás alapú támadások, illetve viharszerű lekérdezések elleni védekezésül.

d) Biztosítani kell a bemeneti információ ellenőrzését *az {Open Web Application Security Project Application Security Verification Standard (ASVS) aktuális verziója;}* dokumentum alapján.

II.18.3. A határok védelme

Mind a belső, mind a külső hálózati szolgáltatókhoz történő hozzáférést a következő módon kell ellenőrizni:

a) **Minden tilos, ami kifejezetten nincs megengedve!** Ez azt jelenti, hogy alaphelyzetben minden forgalmat tiltani kell, majd csak azt megengedni, amelyre valóban szükség van.

b) A belső hálózat irányából az internet irányába kapcsolatot csak azokra a protokollokra/szolgáltatásokra engedélyezünk, amelyre szükség van.

c) Kifejezetten tiltani kell a belső hálózat irányából az internet irányába a levelezési (SMTP) kapcsolatokat. Levelet továbbítani csak a levelező szerveren keresztül szabad.

d) Megfelelő interfészt kell alkalmazni a Hivatal és más szervezet tulajdonában lévő, vagy nyilvános hálózat között.

e) Ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

f) A Hivatal belső hálózatáról Internet kapcsolat kizárólag jóváhagyott tűzfalakon keresztül létesíthető.

g) Biztosítani kell, hogy a Hivatal elektronikus információs rendszerei alapértelmezés szerint ne legyenek elérhetők az Internet felől. Amelyeknél az Internet felöli hozzáférés szükséges igény, ott kizárólag biztonságos és ellenőrzött kapcsolaton keresztül történhet hozzáférés.

h) Minden Internet elérést naplózni kell, annak érdekében, hogy kellő mennyiségű információt lehessen összegyűjteni a szabálytalan internetes tevékenységek detektálása és kiderítése érdekében.

i) Figyelni kell és 1 héten belül telepíteni kell a tűzfal operációs rendszere/firmware-e biztonsági frissítéseit.

j) A tűzfalat úgy kell konfigurálni, hogy az akadályozza és naplózza a port letapogatási próbálkozásokat.

k) A felhasználóknak tilos az Internet felhasználási szabályait és biztonsági beállításait megváltoztatni, illetve megkerülni.

l) A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

m) Az IBF köteles ellenőrizni, hogy a felhasználók számára biztosított az Internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.

n) A Hivatal Hivatali tűzfalát csak a belső hálózatból vagy a konzolról lehet adminisztrálni. A külső hozzáférés nem engedélyezett.

A fentiek végrehajtása érdekében tűzfal biztonsági politikát kell készíteni, mely tartalmazza:

a) a tűzfal kialakítására vonatkozó követelményeket,

b) a tűzfalon engedélyezett portokat, protokollokat és szolgáltatásokat,

c) a tűzfal adminisztrálásával kapcsolatos feladatokat és felelősségi köröket,

d) a tűzfal biztonsági politikában foglaltak ellenőrzését.

II.18.3.1. A hálózati szolgáltatások belső használatának szabályozása

A Hivatal elektronikus információs rendszerében a felhasználók csak azokhoz a hálózati szolgáltatásokhoz férhetnek hozzá, amelyek használata a munkavégzésükhöz feltétlenül szükségesek.

A hálózatokkal és a hálózati szolgáltatásokkal kapcsolatosan az alábbiakat kell figyelembe venni:

a) A felhasználókkal meg kell ismertetni azoknak a hálózatoknak és hálózati szolgáltatásoknak a felsorolását, amelyeket igénybe vehetnek;

b) A hálózati kapcsolatokhoz és szolgáltatásokhoz való hozzáférés védelmére szolgáló óvintézkedések és eljárások tartalmazzanak bejelentkezési védelmet vagy más, az alkalmazások jogosításának ellenőrzésére szolgáló védelmet;

A hálózati szolgáltatások használatával kapcsolatos szabályozást összhangban kell tartani a hozzáféréseket meghatározó követelményekkel.

A Hivatal elektronikus információs rendszerében TILOS modemet csatlakoztatni.

II.18.3.2. Hálózat szegmentálás

A Hivatal hálózatában az infokommunikációs szolgáltatásokat, felhasználókat és elektronikus információs rendszereket szegmentálni kell. A külső felhasználók Internet irányából csak a szükséges elektronikus információs rendszereket érhetik el. A belső hálózatot tűzfal válassza el a többi zónától.

Az Internet és a Hivatal elektronikus információs rendszere közötti hálózati forgalom szűrésére, a lehetőségek korlátozására tűzfalak, tartalomszűrők, illetve meghatározott címekkel a kapcsolat tiltását biztosító megoldások szolgáljanak.

II.18.3.3. A hálózati üzenettovábbítás ellenőrzése

A hálózati üzenettovábbítás ellenőrzését a tűzfalaknak, illetve kapcsolódó tartalomszűrő és címfordító megoldásoknak, valamint azok naplóinak kell biztosítaniuk.

II.18.4. Kriptográfiai kulcs előállítása és kezelése

Kriptográfiai kulcs előállítása és kezelése során a következők szerint kell eljárni:

Szoftveres kulcs esetén a kulcsok előállítása a rendszergazda feladata. A kulcsok létrehozása során meg kell róla győződni, hogy naprakész, megfelelően telepített és konfigurált szoftver- vagy hardverkomponensek kerülnek felhasználásra. Különös figyelmet kell fordítani az igénybe vett véletlenszám-generátor számára biztosított megfelelő entrópia-forrásról. A létrehozás során olyan környezet és tároló vehető igénybe, amelyen az átadás után biztosítható a biztonságos megsemmisítés.

Hardveres kulcs esetén a gyártó ajánlásai alapján kell létrehozni a kulcsot. Amennyiben a kulcs aktiválásához jelszó vagy PIN kód szükséges, úgy gondoskodni kell róla, hogy

a) a PIN/jelszó megfeleljen a jelen IBSZ-ben foglalt jelszóházirendnek, illetve hogy a

b) a kezdeti PIN kódot/jelszót az átvevő megváltoztassa, vagy közvetlenül megadhassa.

Hardveres kulcstárolás esetén gondoskodni kell róla, hogy a kulcstároló eszközről a magánkulcsok ne legyenek exportálhatóak.

A létrehozás és átadás teljes folyamata során biztosítani kell, hogy a kriptográfiai eszközök tartalmát harmadik fél ne ismerhesse meg, arról másolatot, feljegyzést ne készíthessen. (Fájl megosztással szándékon kívül elérhetővé tett szoftveres kulcsok, felügyelet nélkül hagyott hardvereszközök kizárása stb.)

Az átadott eszközök nyilvántartását a rendszergazda végzi.

A kriptográfiai kulcsok cseréje a létrehozás, átadás, megsemmisítés rendje szerint zajlik.

A kriptográfiai kulcsok megsemmisítése során a következők szerint kell eljárni:

a) Amennyiben a megsemmisített kulcs olyan aszimmetrikus kulcspár része, amelyet azonosításra használnak, akkor a kulccsal való hozzáférést logikailag is meg kell szüntetni;

b) amelyet hitelesítésre használnak, úgy a kulcsot a körülményektől függően vissza kell vonni, illetve a regisztrációját meg kell szüntetni.

c) A kulcs, kulcspár megsemmisítése során, hardveres kulcsok esetén a jelen IBSZ adathordozók kezelésére és megsemmisítésére vonatkozó előírásai, szoftveres kulcsok esetén a jelen IBSZ biztonságos adatmegsemmisítésre vonatkozó előírásai alkalmazandóak a kulcs minden előfordulási példánya esetén.

Amennyiben a kulcsról biztonsági másolat készül (DC, boríték, egyéb mentések), úgy a másolatok körültekintő megsemmisítéséről is gondoskodni kell.

A kulcsok megsemmisítését a rendszergazda végzi, erről jegyzőkönyvet vesz fel.

A bizalmi szolgáltatók által biztosított kriptográfiai kulcsok kezelése során a szolgáltató által közzétett ÁSZF alapján kell eljárni.

II.18.5. Kriptográfiai védelem

A Hivatalnak az elektronikus információs rendszereiben az adatok sértetlenségének és bizalmasságának védelmére a vonatkozó mértékadó dokumentumokban biztonságosnak minősített, következő kriptográfiai műveleteket kell alkalmaznia.

a) Szimmetrikus kulcsú titkosítás esetén: AES 128, 192, 256;

b) Aszimmetrikus kulcsú titkosítás: RSA 2048 bit;

c) Elektronikus aláírás: RSA: 2048 bit vagy ECDSA (pLEN 256 bit);

d) Kulcscsere: Diffie-Helmann 2048 bit;

e) Lenyomatolás: SHA1, SHA 2, SHA3 (minimum 256 bit);

f) Jelszótárolás: PBKDF2 alapú hash függvények használata, mint például az scrypt, bcrypt, stb.

Más, egyedi kriptográfiai megoldások akkor alkalmazhatóak, ha:

a) a vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kriptográfiai algoritmusokat és protokollokat használnak;

b) az implementációt külső független szakértő auditálta;

c) alkalmazását az IBF jóváhagyta.

II.18.6. Együttműködésen alapuló informatikai eszközök

A Hivatal elektronikus információs rendszereiben együttműködésen alapuló számítástechnikai eszközt (pl.: kamera, mikrofon) csak akkor lehet aktiválni/használni, ha azt a felhasználó előzőleg jóváhagyta.

II.18.7. Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás) (*)

A Hivatal elektronikus információs rendszereinek működtetése során olyan névfeloldást biztosító megoldást (DNS) kell alkalmazni, mely 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.

II.18.8. Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás) (*)

A Hivatal elektronikus információs rendszereinek működtetése során olyan névfeloldást biztosító megoldást (DNS) kell alkalmazni, mely eredethitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

II.18.9. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén (*)

A névfeloldási szolgáltatás kialakításakor gondoskodni kell a DNS kiszolgálók redundanciájának a megvalósításáról, illetve szét kell választani a belső és a külső szerepköröket.

II.18.10. A folyamatok elkülönítése

A Hivatal elektronikus információs rendszereiben csak olyan modern, gyártó által támogatott operációs rendszerek használhatóak, amelyek biztosítják az elkülönített végrehajtási tartomány fenntartását minden végrehajtó folyamat számára.

II.19. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

A technológiai vhr **RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.19.1. Szabályzat és eljárásrendek

A Hivatal rendszer- és információsértetlenségi vonatkozó szabályzatát az IBSZ jelen fejezete tartalmazza.

II.19.2. Hibajavítás

A rendszerprogramokkal kapcsolatos bármely konfigurálási, hangolási műveletet csak a rendszergazda végezhet. Az alkalmazáson végzendő, annak bármely funkcióját megváltoztató művelethez – beleértve a verzióváltást és egyéb, jelentős beavatkozást igénylő hangolást is - a Jegyző engedélye szükséges.

A rendszergazdának biztosítania kell, hogy a rendszerszoftver naprakész állapotban legyen, és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az üzemeltetők számára.

Az alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni.

A felhasználói adatok és alkalmazások védelme érdekében a szoftverek módosítása (frissítés, verzióváltás) folyamán az alkalmazáshoz és az adatokhoz történő illetéktelen hozzáférést és az illetéktelen próbálkozást meg kell akadályozni. Gondoskodni kell arról, hogy a telepített alkalmazások, fájlok ne károsodjanak, és a követelményeknek megfelelően működjenek.

Új hardverek üzembe állításakor a fentieket kell értelemszerűen alkalmazni.

Gondoskodni kell arról, hogy a munkaállomásokon telepített operációs rendszerek és egyéb segédprogramok naprakészek legyenek.

Gyártói támogatással nem rendelkező operációs rendszerek és egyéb alkalmazások használata tilos.

A rendszergazdának gondoskodnia kell az általa felügyelt elektronikus információs rendszerek rendszerkomponensei sérülékenységeinek figyeléséről.

II.19.2.1. Biztonságkritikus szoftverek

A Hivatalnál a következő szoftverek számítanak biztonságkritikus szoftvernek:

a) tűzfal szoftvere;

b) VPN szoftver;

c) kiszolgáló és kliens oldali kártékony kód elleni védelem;

d) kártékony kód elleni védelem Hivatali menedzsment felülete;

e) spamszűrő szoftver;

f) munkaállomások web böngészői.

A biztonság kritikus szoftverek biztonsági frissítéseit 2 héten belül telepíteni kell.

II.19.2.2. Microsoft termékek biztonsági frissítéseinek telepítése

A Microsoft termékek biztonsági frissítéseinek a telepítéséről a megjelenésüktől számított 2 héten belül gondoskodni kell. A biztonsági frissítéseket a rendszergazdának előzetesen tesztelni kell.

II.19.2.3. Nem Microsoft termékek biztonsági frissítéseinek telepítése

A nem Microsoft termékek frissítését a gyártói ajánlások figyelembe vételével kell elvégezni. A biztonsági frissítések telepítése a rendszergazda feladata.

II.19.3. Kártékony kódok elleni védelem

A Hivatalnak meg kell őriznie az elektronikus információs rendszerek és az információ bizalmasságát, sértetlenségét és rendelkezésre állását a kártékony kódok és a kéretlen üzenetek támadásaival szemben.

A kártékony kódok elleni védekezés során a következőkről kell gondoskodni:

a) Munkaállomások és kiszolgálók esetében memóriában rezidens kártékony kód elleni megoldásokat kell alkalmazni.

b) Hetente egyszer egy teljes körű, ütemezett átvizsgálást kell elvégezni.

c) Kártékony kód elleni megoldás nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.

d) Egyéb infokommunikációs eszközök tekintetében a gyártói ajánlások és a lehetőségek figyelembe vételével törekedni kell a kártékony kódok elleni védekezésre.

e) A kártékony kód elleni alkalmazások adatbázisát automatikusan frissíteni kell.

f) A kártékony kód elleni alkalmazásnak az email-ek csatolmányát ellenőriznie kell, a futtatható állományok szűrését be kell kapcsolni.

g) A hordozható számítógépek esetében az üzemeltetőnek gondoskodnia kell a kártékony kód elleni alkalmazás adatbázisának automatikus frissítéséről, közvetlenül a hordozható számítógép bekapcsolása után.

h) A külső forrásból származó cserélhető adathordozókat használatba vétel előtt automatikus kártékony kód ellenőrzés alá kell vetni.

i) A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal.

j) A kártékony kód felfedezésekor teendő intézkedéseket és a jelentési rendszert szabályozni kell. A rendszergazdának értesítenie kell az IBF-et. A további teendőket az IBF határozza meg.

k) Kártékony kód általi fertőzéskor a munkaállomást haladéktalanul le kell választani a Hivatali hálózatról és így kell megtenni a szükséges vírusirtást, vagy a rendszer újratelepítését.

l) A vírusfertőzésekkel és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell.

II.19.3.1. Vírusriadó

A vírusriadót az IBF javaslatára a Jegyző rendelheti el.

Abban az esetben, ha egyértelműen megállapítható, hogy a tapasztalt jelenségeket vírusfertőzés okozza, és a vírus egy-két gépet fertőzött csak meg, akkor vírusriadót nem szükséges elrendelni. A fertőzött gépeket azonnal le kell kapcsolni a hálózatról, meg kell kísérelni a vírusok kiirtását. Ha ez nem sikerül, akkor vírusriadót kell elrendelni.

Feltétlenül vírusriadót kell elrendelni a következő esetek bármelyikénél:

a) ha a szokásosnál sokkal több vírusincidens történt;

b) a vírusfertőzést magas kockázatúnak értékeli a vírusvédelmi szoftver gyártója;

c) ugyanaz a vírus fordul elő egyszerre kettőnél több gépen, különböző állományokban;

d) valamely számítógépen aktivizálódik a vírus romboló rutinja, vagy a vírus valamilyen effektust (videó, hang stb.) produkál annak ellenére, hogy a vírusadatbázis frissített, a víruskereső motor működött;

e) adatátvitel során, egy számítógépen jelentkező szokványostól eltérő működés, átkerül más számítógépekre is;

f) szerver oldali vírusfertőzés esetén.

A vírusriadó idején a vírus mentesítés szakmai felügyeletét az IBF és a rendszergazda közösen látják el.

II.19.3.2. Teendők vírusfertőzés, vírusriadó esetén

Az IBF feladata a vírus fertőzés kivizsgálásának irányítása, a felelősség megállapítása.

A rendszergazda feladatai:

a) a vírusvédelmi rendszer támogatójának értesítése;

b) a vírus fertőzés következtében szükséges intézkedések koordinálása;

c) a fertőzés tényének és a foganatosított intézkedéseknek a rögzítése;

d) a vírusos számítógép leválasztása a hálózatról;

e) a felhasználók értesítése a vírusról;

f) az e-mail rendszer leállítása, ha emailben terjedő vírusról van szó;

g) a hálózaton terjedő vírus esetén a külső kapcsolat megszakítása;

h) a vírus adatait tartalmazó vírus tudásbázis letöltése és teljes vírusellenőrzés végrehajtása;

i) a fertőzöttség lehetőségeinek feltérképezése, gondolva a hálózaton cserélhető adathordozók által, vagy e-mailen történő fertőzésekre;

j) a kliensek frissítése;

k) manuális vírus ellenőrzés végrehajtása azokon a munkaállomásokon, amelyek megfertőződhettek;

l) amennyiben az a Hivatalon kívülre is terjedhetett, értesíteni kell az érintett szervezeteket;

m) a vírus fertőzés okának kivizsgálása a vírusvédelmi szoftver támogatójával közösen.

II.19.4. Az EIR monitorozása

Az elektronikus információs rendszerek napi üzemeltetéséhez tartozik a működés felügyelete, védelme, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.

Az elektronikus információs rendszerek felügyelete az alkalmazások, az adatbázisok, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg.

Az elektronikus információs rendszer felügyeletének célja, hogy a kibertámadások, vagy a kibertámadásra utaló jelek észlelésre kerüljenek, és feltárásra kerüljön a jogosulatlan lokális, hálózati vagy távoli kapcsolatok és a jogosulatlan használata az elektronikus információs rendszernek.

Automatikus eszközökkel monitorozni kell a tűzfalak, a kiszolgálók, a hálózati aktív eszközök következő erőforrásait és az azokon futó kritikus szolgáltatásokat:

a) éles kiszolgálók merevlemezeinek telítettsége – 80%;

b) memória kihasználtság – 80%;

c) processzor terhelés – 90%;

d) futó szolgáltatások állapota.

Az internet kijáratnál behatolás-detektáló rendszert kell működtetni, melynek jelzéseit folyamatosan figyelni kell és meg kell tenni a szükséges reagálásokat.

A fenti feladatok biztosítása a rendszergazda feladata.

A rendszergazdának ismernie kell a Hivatal rendszereszközeinek, elektronikus információs rendszereinek működését és azok figyelmeztető és hibaüzeneteit. A szükséges reagálásokat tartalmazó leírást tudniuk kell alkalmazni.

A rendszergazdának rendszeresen el kell végeznie azokat a tevékenységeket, amelyek alapján meggyőződhet arról, hogy az elektronikus információs rendszer üzemszerűen működik, így különösen rendszeresen ellenőriznie kell

a) az elektronikus információs rendszerek működőképességét;

b) a vírusdefiníciós állományok naprakészségét;

c) a kártékony kód elleni védelem naplóállományait;

d) az elektronikus információs rendszerek mentésének sikeres lefutását;

e) a monitorozó eszközök riasztásait;

f) a Hivatali tűzfal működőképességét és naplóállományait.

Az üzembiztonság érdekében a kiszolgálók operációs rendszereinek telepítőkészleteit tartalék adathordozón is tárolni kell, valamint az operációs rendszer beállításait rendszeresen menteni kell.

Az üzemeltetési eljárások megfelelőségét az információbiztonsági felülvizsgálatok alkalmával az IBF felülvizsgálja, a szükséges módosításokat átvezetik, a Jegyző pedig jóváhagyja.

II.19.5. Biztonsági riasztások és tájékoztatások (*)

A Hivatalnak az IBF útján folyamatosan figyelemmel kell kísérnie az kiberbiztonsági incidenskezelő Hivatal által kiadott figyelmeztetéseket, riasztásokat, valamint a Hatóság által közzétett értesítéseket.

Az IBF-nek meg kell vizsgálnia, hogy az adott riasztás vagy értesítés érinti-e a Hivatal, illetve annak elektronikus információs rendszereit és szükség esetén belső riasztást kell kiadnia az érintett szerepkörök részére.

A biztonsági események kezelésére vonatkozó szabályokat a jelen IBSZ *{II.10. Biztonsági események kezelése}* fejezete tartalmazza.

II.19.6. Információ kezelése és megőrzése

A kimeneti információk (pl.: nyomtatás) kezelésével és szétosztásával kapcsolatban a Hivatal Iratkezelési Szabályzatával összhangban a következők az előírások:

a) gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről,

b) gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódik,

c) gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat,

d) biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

II.20. ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSE (*)

A technológiai vhr **ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSE** kontrollcsalád ALAP biztonsági osztályára előírt követelményeket az IBSZ jelen fejezete tartalmazza.

II.20.1. Ellátási láncra vonatkozó kockázatmenedzsment szabályzat (*)

A Hivatalnak ki kell dolgoznia, ki kell adnia és meg kell ismertetnie a szervezet által meghatározott személyekkel szerepkörük szerint a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó ellátási láncra vonatkozó kockázatmenedzsment szabályzatot, amely

a) meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá
b) összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.
c) az ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásrendet, amely az ellátási láncra vonatkozó kockázatkezeléséhez kapcsolódó szabályok és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

Ki kell jelölni egy személyt, aki az ellátási láncra vonatkozó kockázatmenedzsment szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

Felülvizsgálja és frissíti az aktuális ellátási láncra vonatkozó kockázatmenedzsment szabályzatot és az ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

A Hivatal a rendelkezése alatt álló EIR-ek, rendszerelemek vagy rendszerszolgáltatások tekintetében szabályzatot dolgoz ki a kutatás-fejlesztés, tervezés, gyártás, beszerzés, szállítás, integráció, üzemeltetés és karbantartás, kivezetés, valamint a selejtezés során felmerülő ellátási lánccal kapcsolatos kockázatok kezelésére.

2 évente felülvizsgálja és frissíti az ellátási lánc kockázatmenedzsment szabályzatát, illetve szükség szerint annak érdekében, hogy kezelje a fenyegetéseket, valamint a szervezeti és környezeti változásokat.

Védeni kell az ellátási lánc kockázatmenedzsment szabályzatát a jogosulatlan közzétételtől és módosítástól.

II.20.2. Ellátási láncra vonatkozó követelmények és folyamatok (*)

A Hivatalnak folyamatot vagy folyamatokat kell kialakítania annak érdekében, hogy azonosítsa és kezelje a gyengeségeket vagy hiányosságokat a meghatározott EIR ellátási láncának elemeiben és folyamataiban, a szervezet által meghatározott ellátási láncért felelős személyekkel együttműködve.

Alkalmazni kell a Hivatal által meghatározott ellátási lánccal kapcsolatos kontrollokat annak érdekében, hogy védje az EIR-t, rendszerelemet vagy rendszer szolgáltatást az ellátási lánccal kapcsolatos kockázatokkal szemben és csökkentse az ellátási lánccal kapcsolatos eseményekből eredő károkat és következményeket.

A Hivatalnak dokumentálnia kell a meghatározott és bevezetett ellátási láncot érintő folyamatokat és kontrollokat a biztonsági szabályzatokban, az ellátási lánc

kockázatmenedzsment szabályzatában és egyéb, a szervezet által meghatározott dokumentumban.

II.20.3. Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók (*)

A Hivatalnak gondoskodnia kell arról, hogy az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák.

II.20.4. Beszerzési stratégiák, eszközök és módszerek (*)

A szervezetnek meg kell határoznia azokat a beszerzési stratégiákat, szerződéses eszközöket és beszerzési módszereket, melyek segítségével védeni, azonosítani és csökkenteni tudja az ellátási láncból eredő kockázatokat.

II.20.5. Értesítési megállapodások (*)

A Hivatalnak megállapodásokat kell kötnie és eljárásokat kell létrehoznia a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő szervezetekkel.

II.20.6. Rendszerek vagy rendszerelemek vizsgálata (*)

A Hivatalnak eseti jelleggel vagy meghatározott gyakorisággal és meghatározott esetekben ellenőriznie kell az EIR-eket vagy rendszerelemeket az esetleges hamisítás felderítése érdekében.

II.20.7. Rendszerelem hitelessége (*)

A Hivatalnak

a) ki kell alakítania és be kell vezetnie a hamisítás elleni szabályokat és eljárásokat, amelyek magukban foglalják a hamisított rendszerelemek észlelését és annak megelőzését, hogy ezek bejussanak az EIR-be; valamint

b) jelentenie kell a hamisított rendszerelemeket és azok forrását a szervezet által meghatározott külső szervezeteknek, illetve a szervezet által meghatározott személyeknek vagy szerepköröknek.

II.20.8. Rendszerelem hitelessége – Hamisítás elleni képzés (*)

A Hivatalnak a meghatározott személyeknek vagy szerepköröknek képzést kell biztosítania a hamisított rendszerelemek (beleértve a hardvert, szoftvert és firmware-t) felismerésére.

II.20.9. Rendszerelem hitelessége – Konfigurációfelügyelet (*)

A Hivatalnak fenn kell tartania a konfiguráció felügyeletét a meghatározott szervizelésre vagy javításra váró, vagy olyan rendszerelemek esetén, amelyeket szervizeltek vagy javítottak, és arra várnak, hogy újból üzembe állítsák őket.

II.20.10. Rendszerelem selejtezése, megsemmisítése (*)

A Hivatal meghatározott technikákkal és módszerekkel selejtezi a meghatározott adatokat, dokumentációkat, eszközöket és rendszerelemeket.

II.21. MELLÉKLETEK

1. számú melléklet – Értelmező Rendelkezések

2. számú melléklet – Kockázatelemzési és kezelési módszertan

3. számú melléklet – Jogosultságigénylési űrlap

4. számú melléklet – Felhasználói Informatikai Biztonsági Házirend

5. számú melléklet – Biztonsági események jelentése

6. számú melléklet – Felhasználói Nyilatkozat

7. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

8. számú melléklet – Titoktartási Nyilatkozat

1. számú melléklet – Értelmező Rendelkezések

Az IBSZ-ben használt, és a gyakorlatban alkalmazott, az információbiztonság tárgykörébe tartozó kifejezések, meghatározások megfelelnek a Kibertv. és jelen IBSZ 4.1 fejezetében meghatározott jogszabályok által használt kifejezéseknek, és értelmezésük is azonos ezekkel.

1. *adat:* az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;
2. *adatfeldolgozás:* az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;
3. *adatfeldolgozó:* az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;
4. *adatkezelés:* az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;
5. *adatkezelő:* az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;
6. *adatkicserélő szolgáltatás:* az elektronikus hírközlésről szóló törvény szerinti fogalom;
7. *adatközponti szolgáltatás:* olyan szolgáltatás, amely Hivatalosított elhelyezést, összeköttetést és működést biztosít adattároló, -feldolgozó és -továbbító információtechnológiai és hálózati berendezések számára, ideértve az energiaellátást és környezeti felügyeletet biztosító létesítményeket és infrastruktúrát is;
8. *adatosztályozás:* a szervezet által az elektronikus információs rendszerben kezelt adatok és információk biztonsági besorolása azok bizalmasságának, sértetlenségének és rendelkezésre állásának szempontjából;
9. *ágazaton belüli kiberbiztonsági incidenskezelő Hivatal:* olyan kiberbiztonsági incidenskezelő Hivatal, amelyet az e törvény hatálya alá tartozó egy vagy több, egy ágazathoz tartozó szervezet az ágazaton belül meghatározott szakterületen előforduló kiberbiztonsági incidenseinek a Hivatalosított és egységes kezelése érdekében üzemeltet;
10. *auditor:* az e törvény szerinti kiberbiztonsági audittevékenység végzésére jogosult, független gazdálkodó szervezet;
11. *behatolásvizsgálat:* olyan sérülékenységvizsgálati módszer, amelynek során az IKT-rendszer, valamint az elektronikus információs rendszer gyenge pontjainak feltárására és kihasználhatóságának ellenőrzésére kerül sor a biztonsági intézkedések elleni rosszindulatú támadások szimulációjával;
12. *belső informatikai biztonsági vizsgálat:* olyan sérülékenységvizsgálati módszer, amelynek során az informatikai rendszer sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik, vagy a belső hálózatban használt eszköz, vagy rendszerelem vizsgálata kerül végrehajtásra;
13. *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;
14. *bizalmi szolgáltatás:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;
15. *bizalmi szolgáltató:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;
16. *biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége;

17. *biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;
18. *digitális szolgáltatás:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;
19. *DNS:* hierarchikusan felépülő elnevezési rendszer, más néven doménnévrendszer, amely lehetővé teszi az internetes szolgáltatások és erőforrások azonosítását, lehetővé téve a végfelhasználók eszközei számára az internetes útvonal-meghatározási és összekapcsolási szolgáltatások igénybevételét e szolgáltatások és erőforrások elérése érdekében;
20. *DNS-szolgáltató:* olyan szervezet, amely a következő szolgáltatások valamelyikét nyújtja a szervezeten kívüli más szervezet vagy személy részére:
    a) *autoritatív DNS-szolgáltatás*: a doménnév – doménnév-regisztrációt végző szolgáltató által kezelt – adatainak lekérdezését közvetlenül lehetővé tevő szolgáltatás, amely a legfelső szintű doménnév-nyilvántartó szolgáltatás része,
    b) *rekurzív DNS-szolgáltatás*: olyan DNS-szolgáltatás, amely a felhasználók doménnév-lekérdezéseit a megfelelő autoritatív DNS-szolgáltatókhoz továbbítja a hierarchikusan felépülő doménnévrendszerben és az autoritatív DNS-szolgáltató által a lekérdezésre adott válaszokat továbbítja a felhasználó részére,
    c) *DNS-gyorsítótárazás*: a doménnév-lekérdezésre adott válaszok átmeneti tárolása és a felhasználói lekérdezéseknek a tárolt doménnévadatok alapján történő kiszolgálása,
21. *doménnév:* az internetes kommunikációhoz használt IP-cím alfanumerikus karakterekből álló megfelelője,
22. *doménnév-regisztrációt végző szolgáltató:* a legfelső szintű doménnév-nyilvántartó által felhatalmazott szolgáltató, amely jogosult domén regisztrálására;
23. *elektronikus hírközlési szolgáltató:* az elektronikus hírközlésről szóló törvény szerinti fogalom;
24. *elektronikus információs rendszer:*
    a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat,
    b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy
    c) az a) és b) alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;
25. *elektronikus információs rendszer biztonsága:* az elektronikus információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;
26. *életciklus:* az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;
27. *esemény:* az elektronikus információs rendszerben bekövetkezett állapotváltozás;
28. *európai kiberbiztonsági tanúsítási rendszer:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 9. pontja szerinti fogalom;
29. *felhasználó szervezet:* Hivatali rendszert vagy Hivatali szolgáltatást igénybe vevő szervezet;
30. *felhőszolgáltatás:* olyan digitális szolgáltatás, amely önkiszolgáló módon történő hálózati hozzáférést tesz lehetővé igény szerint méretezhető, megosztott fizikai vagy virtuális erőforrások rugalmas készletéhez;

31. *felhőszolgáltató:* felhőalapú számítástechnikai szolgáltatást nyújtó szervezet;
32. *gyártó:* az IKT-termék gyártója, IKT-szolgáltatás nyújtója, valamint IKT-folyamat gyártója vagy nyújtója;
33. *használatbavétel:* az elektronikus információs rendszer adatokkal való feltöltése és rendeltetésszerű használatának megkezdése;
34. *honvédelmi célú elektronikus információs rendszer:*
    a) a honvédelmi szervezetek, a honvédelemért felelős miniszter fenntartói irányítása alá tartozó, honvédségi szervezetnek nem minősülő többcélú szakképző intézmény, a honvédelemért felelős miniszter tulajdonosi joggyakorlása alá tartozó gazdasági társaságok, valamint jogszabály szerint a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok elektronikus információs rendszereinek összessége, amely ágazatspecifikus módon támogatja a honvédelmi ágazaton belüli és ágazatok közötti működést,
    b) az ország védelme és biztonsága szempontjából jelentős honvédelmi ágazaton belüli szervezet és infrastruktúra elektronikus információs rendszerei,
    c) az ország védelme és biztonsága szempontjából jelentős kettős kijelöléssel nem érintett honvédelmi szervezet és honvédelmi infrastruktúra elektronikus információs rendszerei, valamint
    d) a honvédelmi kiberbiztonsági hatóság által alapvető vagy fontos szervezetként azonosított szervezet elektronikus információs rendszere;
35. *honvédelmi kiberbiztonsági incidenskezelő Hivatal:* a Kibertv. 63. § (2) bekezdése szerint kijelölt szerv;
36. *ideiglenes hozzáférhetetlenné tétel:* az elektronikus adathoz való hozzáférés ideiglenes megakadályozása;
37. *IKT-folyamat:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 14. pontjában meghatározott fogalom;
38. *IKT-szolgáltatás:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 13. pontjában meghatározott fogalom;
39. *IKT-termék:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 12. pontjában meghatározott fogalom;
40. *jelentős kiberbiztonsági incidens:*
    a) a közvetlenül alkalmazandó európai uniós jogi aktusban ekként meghatározott kiberbiztonsági incidens,
    b) közvetlenül alkalmazandó európai uniós jogi aktus hiányában az olyan kiberbiztonsági incidens, amely
        ba) a szervezet üzleti szolgáltatásának vagy a szervezet által nyújtott szolgáltatásnak legalább 5%-os csökkenésével vagy a szervezet éves bevételének legalább 5%-os kiesésével jár vagy fenyeget;
        bb) súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek; vagy
        bc) jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett, vagy képes érinteni;
41. *jelentős kiberfenyegetés:* olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni hátrányt vagy kárt okozva súlyos hatást gyakorolhat egy szervezet elektronikus információs rendszereire, vagy a szervezet szolgáltatásainak felhasználóira;

42. *képviselő:* Magyarországon letelepedett minden olyan természetes vagy jogi személy, akit vagy amelyet kifejezetten kijelöltek arra, hogy valamely, Magyarországon nem letelepedett szervezet nevében eljárjon, és akihez vagy amelyhez a kiberbiztonsági hatóság, vagy a kiberbiztonsági incidenskezelő Hivatal az adott szervezet helyett fordulhat;
43. *kiberbiztonság:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 1. pontjában meghatározott fogalom;
44. *kiberbiztonsági audit:* az elektronikus információs rendszerek biztonsági osztályba sorolása, valamint a biztonsági osztályba sorolás szerinti védelmi intézkedések megfelelőségének ellenőrzése;
45. *kiberbiztonsági hatóság:* a 23. § (1) bekezdés a) és b) pontja, valamint (2) bekezdése szerinti hatóság;
46. *kiberbiztonsági incidens:* olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;
47. *kiberbiztonsági incidenskezelés:* minden olyan tevékenység és eljárás, amelynek célja a kiberbiztonsági incidens megelőzése, észlelése, elemzése és elszigetelése vagy a kiberbiztonsági incidensre való reagálás és a kiberbiztonsági incidenst követően a működés helyreállítása;
48. *kiberbiztonsági incidenskezelő Hivatal:* a Kibertv. 63. § (1) és (2) bekezdése szerinti szerv;
49. *kiberbiztonsági incidensközeli helyzet:* olyan esemény, amely veszélyeztethette volna az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok, vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;
50. *kiberfenyegetés:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 8. pontjában meghatározott fogalom;
51. *kiber-fizikai rendszer:* olyan programozható elektronikus információs rendszerek, amelyek kölcsönhatásba lépnek a fizikai környezettel vagy kezelik a fizikai környezettel kölcsönhatásba lépő eszközöket. Ezek az elektronikus információs rendszerek közvetlenül fizikai változást érzékelnek vagy idéznek elő az eszközök, folyamatok és események megfigyelésével vagy vezérlésével;
52. *kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató:* olyan kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, amely a kiberbiztonsági kockázatok kezelését végzi vagy azzal összefüggő szolgáltatást nyújt;
53. *kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató:* olyan szervezet, amely az IKT-termék, hálózat, infrastruktúra, alkalmazás vagy bármely más elektronikus információs rendszer telepítésével, kezelésével, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt a szolgáltatást igénybe vevő telephelyén vagy távolról;
54. *kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának, bekövetkezési valószínűségének és az ez által okozott kár nagyságának a függvénye;
55. *kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének, fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
56. *kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása és az intézkedések végrehajtása;

57. *kockázatmenedzsment keretrendszer:* olyan strukturált, ugyanakkor rugalmas megközelítés és szervezeti folyamatok összessége, amely integrálja a kiberbiztonsággal kapcsolatos kockázatkezelési tevékenységeket a rendszerfejlesztési életciklusban a kockázatokkal arányos védelmi intézkedések azonosításán, bevezetésén, értékelésén, működtetésén és nyomon követésén keresztül az új és már használatban lévő rendszerek fenyegetettségeinek folyamatos felderítése, és kockázatainak hatékony kezelése érdekében;
58. *közigazgatási szerv:* Kibertv. 1. melléklet 1–13. pontja szerinti szervezet;
59. *közösségimédia-szolgáltatási platform:* olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg, fedezzenek fel és kommunikáljanak egymással;
60. *Hivatali rendszer:* egyes állami, önkormányzati feladatok ellátását segítő, zárt ügyfélkör számára Hivatalosítottan fejlesztett vagy működtetett elektronikus információs rendszer, amelyen keresztül megvalósított funkciókat egy adott intézményi körben kötelezően vagy opcionálisan vesznek igénybe a felhasználó szervezetek;
61. *Hivatali szolgáltatás:* a központi szolgáltató által kötelezően vagy egyedi igény alapján biztosítandó szolgáltatás;
62. *Központi szolgáltató:* olyan szervezet, amely állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal nyújt informatikai és elektronikus hírközlési szolgáltatást;
63. *kutatóhely:* a tudományos kutatásról, fejlesztésről és innovációról szóló törvény szerinti kutatóhely – az oktatási intézmények kivételével –, amelynek elsődleges célja alkalmazott kutatás vagy kísérleti fejlesztés folytatása a kutatás eredményeinek kereskedelmi célokra való hasznosítása céljából;
64. *legfelső szintű doménnév-nyilvántartó:* olyan szervezet, amelyre egy meghatározott legfelső szintű domént bíztak és amely felelős egyrészt a legfelső szintű domén kezeléséért – ideértve a legfelső szintű domén alatti doménnevek nyilvántartásba vételét –, másrészt a legfelső szintű domén technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a legfelső szintű doménzónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezeknek az üzemeltetési tevékenységeknek bármelyikét maga a szervezet végzi vagy azokat kiszervezi, kivéve azokat az eseteket, amikor a legfelső szintű doménneveket a nyilvántartó kizárólag saját használatra veszi igénybe;
65. *megfelelőségértékelés:* az az értékelési eljárás, amely bizonyítja, hogy egy IKT-termékkel, IKT-folyamattal, IKT-szolgáltatással kapcsolatos, meghatározott követelmények teljesültek;
66. *megfelelőségértékelő szervezet:* a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló, 2008. július 9-i 765/2008/EK európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom;
67. *megfelelőségi nyilatkozat:* a gyártó vagy a szolgáltató által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek;
68. *megfelelőségi önértékelés:* az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom;
69. *mérföldkő:* az európai uniós forrásból finanszírozott Hivatali rendszer fejlesztése esetén a Helyreállítási és Rezilienciaépítési Eszköz létrehozásáról szóló, 2021. február 12-i (EU) 2021/241 európai parlamenti és tanácsi rendelet 2. cikk 4. pontja és az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alap Pluszra, a Kohéziós Alapra, az Igazságos Átmenet

Alapra és az Európai Tengerügyi, Halászati és Akvakultúra-alapra vonatkozó közös rendelkezések, valamint az előbbiekre és a Menekültügyi, Migrációs és Integrációs Alapra, a Belső Biztonsági Alapra és a határigazgatás és a vízumpolitika pénzügyi támogatására szolgáló eszközre vonatkozó pénzügyi szabályok megállapításáról szóló, 2021. június 24-i (EU) 2021/1060 európai parlamenti és tanácsi rendelet 2. cikk 4. pontja szerinti, valamint a fejlesztésekre irányuló egyéb projektek esetén a projektben meghatározott fogalom;

70. *minősített bizalmi szolgáltatás:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

71. *minősített bizalmi szolgáltató:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

72. *műszaki előírás:* az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendelet (a továbbiakban: 1025/2012/EU rendelet) 2. cikk 4. pontjában meghatározott fogalom;

73. *műveleti célú elektronikus információs rendszer:*

a) a rendvédelmi szervek és a nemzetbiztonsági szolgálatok számára törvényben meghatározott közbiztonsági, nemzetbiztonsági feladatok ellátása érdekében használt elektronikus információs rendszer és
b) a honvédségi szervezetek által, a törvényben meghatározott katonai műveleti feladatok – így különösen közvetlen művelettámogatás, -tervezés, -vezetés, helyzetkövetés – ellátása érdekében használt elektronikus információs rendszer;

74. *nagyszabású kiberbiztonsági incidens:* olyan kiberbiztonsági incidens, amely olyan mértékű zavart okoz, amely meghaladja Magyarországnak az arra való reagálási képességét, vagy amely Magyarországra és legalább még egy másik országra jelentős hatást gyakorol;

75. *nem privát felhőszolgáltatás:* olyan szolgáltató által nyújtott felhőszolgáltatás, amelyet a szolgáltató bárki számára elérhető módon vagy kizárólag a szervezetek egy meghatározott köre számára nyújt;

76. *nemzeti kiberbiztonsági incidenskezelő Hivatal:* az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, kiberbiztonsági incidensekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal rendelkezik [európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

77. *nemzeti kiberbiztonsági tanúsítási rendszer:* IKT-termékek, IKT-szolgáltatások és IKT-folyamatok tanúsítására, megfelelőségértékelésére Magyarországon alkalmazandó, az európai kiberbiztonsági rendszerek elvei alapján kidolgozott és a tanúsító hatóság által meghatározott szabályok, műszaki követelmények, szabványok és eljárások átfogó rendszere;

78. *nemzeti kiberbiztonsági stratégia:* a kiberbiztonság területén követendő stratégiai célokat és prioritásokat, valamint a megvalósításukhoz szükséges irányítási intézkedéseket meghatározó dokumentum;

79. *nemzeti kiberbiztonsági tanúsítvány:* olyan független harmadik fél által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek;

80. *nemzeti válságkezelési terv:* az (EU) 2022/2555 európai parlamenti és tanácsi irányelv alapján a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti terv, amely meghatározza a nagyszabású kiberbiztonsági események és válságok kezelésének célkitűzéseit és szabályait;
81. *online keresőprogram:* az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról szóló, 2019. június 20-i (EU) 2019/1150 európai parlamenti és tanácsi rendelet 2. cikk 5. pontjában meghatározott fogalom;
82. *online piactér:* olyan szolgáltatás, amely a kereskedő által vagy a kereskedő nevében működtetett szoftvert, többek között weboldalt, valamely weboldal egy részét vagy valamely alkalmazást használ, és amelynek révén a fogyasztók távollevők közötti szerződést köthetnek más kereskedőkkel vagy fogyasztókkal;
83. *regisztrált felhasználói jogosultság:* a biztonsági vizsgálatot végző személy számára a sérülékenységvizsgálat elvégzése érdekében célzottan létrehozott felhasználói jogosultság;
84. *rendelkezésre állás:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;
85. *sebezhetőség:* IKT-termék, -szolgáltatás, -folyamat gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti az IKT-termék, -szolgáltatás, -folyamat bizalmasságát, sértetlenségét vagy rendelkezésre állását;
86. *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, azaz hiteles, valamint a származás ellenőrizhetőségét, bizonyosságát, azaz letagadhatatlanságát is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;
87. *sérülékenység:* az elektronikus információs rendszer gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti egy elektronikus információs rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását;
88. *sérülékenységkezelési terv:* a sérülékenységek megszüntetésére irányuló tervdokumentum;
89. 89. *sérülékenységvizsgálat:* sérülékenységmenedzsment eszköz vagy módszer, amely során informatikai rendszerek, hardverek és szoftverek biztonsági szempontból történő átvizsgálása zajlik, az ellenőrzést automatizált eszközökkel és közvetlen, szakértő által végzett vizsgálatokkal hajtják végre;
90. *szabvány*: az 1025/2012/EU rendelet 2. cikk 1. pontjában meghatározott fogalom;
91. *szervezet:* állami szerv vagy állami szervezet, a Polgári Törvénykönyvről szóló törvény szerinti jogi személy, jogi személyiség nélküli szervezet;
92. *támogató rendszer: a* Kibertv. 1. § (1) bekezdés a)–c) pontja szerinti szervezet alapfeladatainak ellátásában közvetlenül nem részt vevő elektronikus információs rendszer, amely szükséges azon rendszerek működéséhez, amelyek alapfeladatot látnak el;
93. *tanúsítás:* független harmadik fél által végzett megfelelőségértékelési tevékenység;
94. *tartalomszolgáltató hálózat szolgáltatója:* a digitális tartalmak és szolgáltatások széles körű, akadálymentes és gyors rendelkezésre állását biztosító, földrajzilag elosztott szerverek hálózatának szolgáltatója;
95. *távoli sérülékenységvizsgálat:* olyan sérülékenységvizsgálat, amelynek során
    a) az elektronikus információs rendszer internet felőli, külső sérülékenységvizsgálatára kerül sor, amelynek keretében az interneten fellelhető, nyilvános adatbázisokban való szabad keresés, célzott információgyűjtés, valamint az elérhető számítógépek szolgáltatásai sebezhetőségének feltérképezése történik,

b) automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei, vagy
c) a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik;

96. *továbbfejlesztés:* az érintett, már működő elektronikus információs rendszer olyan mértékű fejlesztése, amely funkcionalitásának érdemi megváltozásával jár, vagy védelmének elvárt erősségére hatással van;

97. *üzemeltetési kiberbiztonsági incidens:* olyan kiberbiztonsági incidens, amely az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált, vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását nem szándékoltan csökkenti vagy megszünteti;

98. *üzemeltető:* az a természetes személy, jogi személy, jogi személyiség nélküli szervezet vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

99. *zárt, teljes körű, folytonos és a kockázatokkal arányos védelem:* az elektronikus információs rendszer olyan védelme,

a) amely az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósul,
b) amely az elektronikus információs rendszer valamennyi elemére kiterjed,
c) amely az összes számításba vehető fenyegetést, veszélyt figyelembe veszi, valamint
d) amelynek költségei arányosak a fenyegetések által okozható károk értékével.

KOCKÁZATELEMZÉSI ÉS KEZELÉSI MÓDSZERTAN

A jelen dokumentum célja, hogy a jelen IBSZ *{II.16.3.* Kockázatelemzés*}* fejezetében foglalt követelmények végrehajtásának módját leírja.

1. VAGYONLELTÁR

Az elektronikus információs rendszerekre ható fenyegetettségek különbözőek, attól függően, hogy az elektronikus információs rendszer melyik összetevőjét fenyegetik.

A fenyegetettségek megfelelő azonosítása érdekében létre kell hozni és értelemszerűen fel kell tölteni a következő vagyonelem csoportokat a Hivatal vagyonelemeivel:

a) környezeti infrastruktúra;
b) hardver;
c) szoftver;
d) adatok;
e) dokumentumok;
f) humán erőforrások.

2. HELYZETFELMÉRÉS

Az információbiztonsági kockázatelemzés elvégzéséhez fel kell mérni, meg kell ismerni az elektronikus információs rendszereket és azok környezetét, valamint azok jelenlegi információbiztonsági szintjét.

A következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:

a) Adminisztratív védelmi intézkedések
    i. A Hivatalra vonatkozó jogszabályok, szabályzatok;
    ii. Az elektronikus információs rendszerre vonatkozó szabályzatok;
    iii. Szerződések, külső felek kezelése;
    iv. Alkalmazásfejlesztés, változáskezelés;
    v. Jogosultságigénylés;
    vi. Biztonsági események kezelése;
    vii. Üzemeltetési eljárások;
    viii. Szervizelés, eszközcsere, selejtezés.
b) Logikai védelmi intézkedések
    i. Mentési megoldások;
    ii. Kártékony kód elleni védekezés;
    iii. Biztonsági frissítések telepítése,
    iv. Hálózat felépítése;
    v. Biztonsági rendszerek;
    vi. Kriptográfiai megoldások.
c) Fizikai biztonság

i. Beléptetés;
ii. Számítógépterem kialakítása;
iii. Épületben történő közlekedés;
iv. Irodák kialakítása, tiszta asztal, üres képernyő politika.

3. GYENGE PONTOK MEGHATÁROZÁSA

A helyzetfelmérés alapján megszerzett információk birtokában meg kell határozni az egyes vagyonelemek gyenge pontjait.

4. FENYEGETETTSÉGEK ELEMZÉSE

Az egyes vagyonelemek gyenge pontjaira bizonyos fenyegetettségek hatnak.

Az informatikai erőforrásokra ható fenyegetettségek vagy fenyegető tényezők (például: üzleti hírszerzés, rosszindulatú hackerek, természeti katasztrófák) mindig a sérülékeny pontokon keresztül fejtik ki hatásukat, így az ellenük való védekezés legfőbb eleme a sérülékenységek azonosítása és megszüntetése.

Az egyes vagyonelemek gyenge pontjait és fenyegetettségeit a technológiai vhr 3. sz. mellékletében rögzített fenyegetések katalógusa alapján kell azonosítani.

5. SÉRÜLÉKENYSÉGEK ELEMZÉSE

A sérülékenység egy bizonyos gyenge pont kihasználása a rá ható fenyegetettség által. Meg kell vizsgálni, hogy a beazonosított gyenge pontokon keresztül mely fenyegetettségek tudják kifejteni a káros hatásukat.

6. KÁRÉRTÉK SZINTEK KIALAKÍTÁSA, KÁROK RÁVETÍTÉSE A VAGYONELEMEKRE

A következő kárérték szintek kerültek meghatározásra:

Kár mértéke	Adatvédelem	Ügymenet-folytonosság megszakadása	Társadalmi-politikai hatás	Közvetett vagy közvetlen anyagi kár	Személyi sérülés
1. Jelentéktelen kár	Az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot.		Nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható.	A közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen.	
2. Csekély kár	Személyes adat sérülhet.	Az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat vagy elektronikus információs rendszer sérülhet.	A lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;	A közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.	
3. Közepes kár	Különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek; az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat		A lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek.	A közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.	

	kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet.				
4. Nagy kár	Különleges személyes adat nagy mennyiségben sérülhet.	Az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet.	A káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni.	A közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.	Személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket).
5. Kiemelkedően nagy kár	Különleges személyes adat kiemelten nagy mennyiségben sérülhet; a nemzeti adatvagyon helyreállíthatatlanul megsérülhet.	Az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet.	A lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.	A közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.	Emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be.

A kockázatok megállapításához az elektronikus információs rendszerek vagyonelemeire rá kell vetíteni a kárérték szinteket.

7. A BEKÖVETKEZÉSI VALÓSZÍNŰSÉGEK MEGHATÁROZÁSA

Következő lépésként meg kell becsülni a sérülékenységek bekövetkezési valószínűségét.

A bekövetkezési valószínűséghez a következő értékeket kell használni:

- „5” - bármikor bekövetkezhet;
- „4" – 1 hónapon belül várható az előfordulás;
- „3" – egy hónapon túl, de 6 hónapon belül várható az előfordulás;
- „2” – ritka: fél éven túl, de 1 éven belül várható az előfordulás;
- „1" – nagyon ritka: egy ében belül nem várható az előfordulás.

8. KOCKÁZATOK MEGHATÁROZÁSA

Az információbiztonsági kockázatokat a sérülékenység bekövetkezésének a valószínűsége és az okozott kár szorzata fogja megadni.

A kockázatok minősítéséhez a következő kockázati mátrixot kell definiálni:

		Bekövetkezési valószínűségek				
		1	**2**	**3**	**4**	**5**
Kárértékek	**5**	A	K	M	NM	NM
	4	A	K	M	NM	NM
	3	NA	A	K	M	M
	2	NA	A	A	K	K
	1	NA	NA	NA	A	A

A kockázatok jelölése a következő:

- NA - Nagyon alacsony;
- A – Alacsony;
- K – Közepes;
- M – Magas;
- NM - Nagyon magas.

9. ELVISELHETŐ KOCKÁZATOK MEGHATÁROZÁSA

A Hivatal azt a döntést hozta, hogy minden közepes, illetve közepesnél nagyobb kockázatot kezelni kíván.

Ennek megfelelően a toleranciamátrix a következő:

		Bekövetkezési valószínűségek				
		1	**2**	**3**	**4**	**5**
Kárértékek	**5**	T	NT	NT	NT	NT
	4	T	NT	NT	NT	NT
	3	T	T	NT	NT	NT
	2	T	T	T	NT	NT
	1	T	T	T	T	T

A táblázatban alkalmazott jelölések értelmezése a következő:

- T – Tolerálható;
- NT – Nem tolerálható.

10. KOCKÁZATOK KEZELÉSE

A nem tolerálható kockázatokat kezelni kell. A Hivatal a kockázatokat a következőképpen kezeli:

a) Megfelelő intézkedésekkel csökkenti a fenyegetés bekövetkezési gyakoriságát vagy hatását (Kockázat csökkentés);
b) Tudatosan, a következményeket felmérve elfogadja a kockázatot (Kockázat elfogadás);
c) Elkerüli a kockázatot azáltal, hogy az érintett tevékenységet felfüggeszti (Kockázat elkerülés);
d) Áthárítja a kockázatot például biztosítással, vagy megfelelő beszállítói szerződésekkel. (Kockázat áthárítás).

11. KOCKÁZATCSÖKKENTŐ INTÉZKEDÉSEK

A PreDeCo elv alapján a kockázatcsökkentés három szemszögből közelíthető meg:

a) Megelőző jellegű (preventív kontrollok)

   A hibák, gyengeségek, sérülékenységek, illetve ezek kihasználására való lehetőségek kiküszöbölése.

b) Korlátozó vagy javító (korrektív kontrollok)

   Egy veszély hatását csökkentő, enyhítő óvintézkedések, további tevékenységek szükségessége nélkül.

c) Észlelő és reagáló (detektív kontrollok)

A sebezhetőségek támadásának észlelése, ártalmas kihatások enyhítésére, illetve válaszreakciók kidolgozása.

12. INTÉZKEDÉSI TERV

Az el nem viselhető kockázatok kezelésére a Hivatalnak intézkedési tervet kell készítenie az egyes feladatok mellé rendelt felelős, határidő és esetleg költség feltüntetésével.

Az intézkedései tervet az IBF készíti elő a rendszergazda bevonásával és a Jegyző hagyja jóvá.

3. számú melléklet – Jogosultságigénylési űrlap

Hozzáférési jogok igénylése űrlap

Iktatószám:

JOGOSULTSÁGIGÉNYLŐ ADATAI

Igénylő neve: …….
Szervezeti egység: ……
Telefon: ……
E-mail: …….....

Igényelt művelet

Elektronikus információs rendszer megnevezése:.....

Jogosultság kezdete: …… Jogosultság vége: ……..

Új jogosultság
Jogosultság törlése
Jogosultság módosítása

Egyéb:……
……
…….

INDOKLÁS

A jogosultságigényléshez kapcsolódó feladatellátás megnevezése:
……
……

……..
Kelt: …… igénylő aláírása

Munkahelyi vezetői jóváhagyás

Vezető: ……..
Beosztása: …….. …..……..
Kelt: …….. vezető aláírása

Adatgazdai jóváhagyás

Adatgazda: …….. …….
Kelt …… adatgazda aláírása

A jogosultságot beállító aláírása

Rendszergazda: …….. …….
Kelt …… rendszergazda aláírása

Felhasználói Informatikai Biztonsági Házirend

1. ÁLTALÁNOS RÉSZ

1.1. A Felhasználói Informatikai Biztonsági Házirend célja

A Felhasználói Informatikai Biztonsági Házirend (a továbbiakban: FIBH) célja, hogy a Sárbogárdi Polgármesteri Hivatal (továbbiakban: a Hivatal) elektronikus információs rendszereinek felhasználói részére előírja az információbiztonsági előírások rájuk vonatkozó részét.

A Hivatal elektronikus információs rendszereinek védelme érdekében a Hivatal kidolgozta az Informatikai Biztonsági Szabályzatát.

Az Informatikai Biztonsági Szabályzat (továbbiakban: az IBSZ) tartalmazza valamennyi információbiztonsággal kapcsolatos szabályt, melynek betartásával az érintettek által elvárt szinten tartható a Hivatal elektronikus információs rendszereinek és az azokban kezelt adatok biztonsága.

Az IBSZ számos olyan védelmi intézkedést tartalmaz, amely közvetlenül nem kapcsolódik a Hivatal felhasználóihoz, ezért a jelen FIBH-nak az is célja, hogy egy kivonatot adjon az IBSZ felhasználókra vonatkozó előírásairól, illetve tovább értelmezze és érthető módon kommunikálja az IBSZ-ben magasabb szinten meghatározott követelményeket.

1.2. A FIBH általános követelményei

A FIBH előírásainak alkalmazása, betartása, illetve betartatása, a jelen IBSZ *{I.2.1. Szervezeti személyi* hatály*}* **pontban megjelöltek számára kötelező. A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. A FIBH el nem olvasása vagy nem ismerete nem mentesít a felelősség alól.**

Az információbiztonsági előírások betartása megvédi a Hivatalt és a jelen IBSZ *{I.2.1. Szervezeti személyi* hatály*}* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák a FIBH előírásait.

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ *{6. számú melléklet – Felhasználói Nyilatkozat}* mellékletében található nyilatkozat aláírása után lehet használatba venni.

A Hivatal a FIBH-t az IBSZ-szel együtt folyamatosan fejleszti és tökéletesíti.

2. BEVEZETÉS

A Hivatal által kezelt információk érzékenysége miatt azok védelme, azaz bizalmas kezelése, sértetlensége, valamint megfelelő szintű rendelkezésre állása kritikus tényező.

A Hivatal elvégezte a jogszabályok által előírt módon az elektronikus információs rendszereinek biztonsági osztályba sorolását, melynek során valamennyi elektronikus információs rendszert besorolta egy három elemből álló skálán. Az elektronikus információs rendszer biztonsági osztálya adja meg a védelem elvárt szintjét.

A Hivatali ügyviteli folyamatok működése nagymértékben az elektronikus információs rendszereire épül, így ezek kiesése, vagy megsemmisülése esetén a Hivatal egyes funkciói működésképtelenné válhatnak, valamint a Hivatal által kezelt érzékeny információk illetéktelen kezekbe kerülhetnek.

A Hivatal elektronikus információs rendszereinek minden felhasználója személyes felelősséggel tartozik a munkájával kapcsolatban a birtokában lévő, illetve a tudomására jutott információk megfelelő kezeléséért, a biztonsági szabályok betartásáért.

3. A FELHASZNÁLÓ JOGAI, KÖTELESSÉGEI ÉS FELELŐSSÉGE

A felhasználóknak az elektronikus információs rendszerek használata során a következők a jogaik, kötelezettségeik és felelősségeik.

3.1. A felhasználó jogai

A felhasználó jogosult:

a) a számára biztosított infokommunikációs eszközök, szoftverek üzemszerű használatára;

b) a beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére;

c) információbiztonsági képzésre;

d) a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftverek használatához támogatást kérni;

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

3.2. A felhasználó kötelessége

Az információk védelmét azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata, életciklusa során biztosítani kell.

Amennyiben a felhasználó olyan adatokhoz fér hozzá, amelyek kezelésében nem illetékes, a hibát jeleznie kell munkahelyi vezetőjének.

Valamennyi alkalmazott köteles azonnal értesíteni a rendszergazdát minden olyan körülményről, ami az informatikához kapcsolódó tevékenység fennakadásához, megszakadásához vezethet. A rendszergazda szükség esetén értesíti az információbiztonsági felelőst, aki megteszi a további, szükséges intézkedéseket.

Valamennyi információbiztonsággal kapcsolatos észrevételt vagy szabályszegésre vonatkozó feltételezést haladéktalanul jelenteni kell az információbiztonsági felelősnek.

Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosítót, jelszót, eToken-t, kulcsot, vagy bárminemű egyéb, a Hivatal erőforrásaihoz hozzáférést biztosító eszközt.

A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással. A hozzáférési kódok a rendszergazdáknak sem adhatók ki és a rendszergazdáknak nincs is joga ezeket elkérni.

Az információbiztonsági hiányosságok megelőzése céljából a felhasználók kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére, és a tapasztalatokat a további problémák elkerülésében felhasználni.

Az információbiztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban a felhasználó köteles együttműködni a kivizsgálókkal.

A Hivatal infokommunikációs eszközei és elektronikus információs rendszerei kizárólag Hivatali munkavégzés céljából használható, azok magáncélú használata tilos!

A Hivatal a vonatkozó adatvédelmi jogszabályok figyelembevételével jogosult a felhasználó hivatalos elektronikus levelezését és internetforgalmát vizsgálni.

A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, jelszavak kipróbálása, illetve ezek kísérlete is.

A Hivatalnál az alkalmazottak csak a Hivatal tulajdonát képező informatikai eszközöket és engedélyezett szoftvereket használhatják. Ettől eltérni csak a Jegyző írásbeli engedélyével lehet.

A rendszergazdát kivéve, tilos a Hivatal számítógépeire szoftvereket telepíteni és azokat futtatni.

Kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett.

A nyomtatásra, lapolvasásra, fénymásolásra, faxolásra alkalmas készülékek, multifunkcionális eszközök használatánál ügyelni kell arra, hogy:

a) az érzékeny információt tartalmazó nyomtatványok ne maradjanak a készülékben;

b) illetéktelenek ne férhessenek hozzá, mert belső tárolóikban tárolódott üzenetek visszahívhatók, így illetéktelenek kezébe kerülhetnek;

c) véletlen vagy szándékos átprogramozás során az üzenetek egy nem megfelelő számra kerülhetnek;

d) félretárcsázás vagy hibásan tárolt szám miatt az üzenetek illetéktelen személyhez kerülnek.

3.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a szabályok betartásáért;

b) a birtokában lévő, vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért;

c) a személyére szóló és védett területre belépést biztosító kártyájának/kártyáinak védelméért és át nem ruházásáért;

d) az elektronikus információs rendszerben végzett műveletekért;

e) a Hivatal infokommunikációs eszközeinek (számítógép, nyomtató, scanner, stb.) szakszerű kezeléséért;

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

4. AZ INFORMÁCIÓ KEZELÉSÉNEK SZABÁLYAI

4.1. Munkaállomások hozzáférés védelme

A felhasználó munkaállomást csak saját azonosítójával és jelszavával belépve használhat. Harmadik fél csak a munkaállomás nevesített felhasználója vezetőjének előzetes írásbeli engedélyével használhat munkaállomást, ebben az esetben is a személyesen hozzárendelt azonosító használatával. Hibaelhárítás vagy támogatás esetén a rendszergazda saját azonosítójával a felhasználó engedélyével a felhasználó munkaállomására beléphet.

A felhasználónak sem helyi, sem hálózati rendszergazdai jog nem adható!

4.2. A hozzáférés kiosztás folyamata

Az informatikai rendszerekbe belépést lehetővé tevő azonosítót a vezető igényli a felhasználóknak, az IBSZ *{II.3.4. Hozzáférési jogok igénylésének eljárásrendje}* fejezetében leírt folyamat szerint.

A hálózati belépést lehetővé tevő azonosítót és a kezdeti jelszót a rendszergazda személyesen vagy telefonon adja át az új felhasználónak. Az átadás során a rendszergazda az azonosító használatáról, a kezdeti jelszó megváltoztatásáról és az egyéb testre szabási lépésekről oktatásban részesíti a felhasználót.

4.3. Hálózati hozzáférés, hozzáférés az egyes alkalmazói programokhoz

A Hivatal vezetése felügyeli az elektronikus információs rendszerek használatát a visszaélések megakadályozására és jogosult az elektronikus információs rendszer használatát ellenőrizni.

A Hivatal infokommunikációs eszközein működtetett szoftvereket és alkalmazói rendszereket a felhasználó a számára beállított jogosultságnak megfelelően használhatja az alábbiak szerint:

a) A felhasználó a számítógépbe/hálózati szolgáltatások eléréséhez személyre szóló azonosítót és jelszót kap, mely a belépéshez szükséges bizalmas információkat tartalmaz.

b) Az azonosító és a megfelelő erősségű és titokban tartott jelszó használatával a belépő védelemmel rendelkezik a nevében történő visszaélések ellen, ezért a személyre szóló azonosítót és jelszavát szigorúan védeni kell, és a kezdeti jelszót első bejelentkezéskor meg kell változtatni.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

a) A jelszó legalább 12 karakter hosszú legyen, és tartalmaznia kell kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

b) a jelszavakat 365 naponta meg kell változtatni;

c) az előző jelszavak újra használatát 12 alkalommal kerülni kell.

A felhasználói jelszavak alkalmazásakor az alábbi szabályokat kell betartani:

a) a felhasználó a jelszavát köteles titokban tartani;

b) a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az informatikai rendszerben;

c) a felhasználói jelszót TILOS leírni;

d) ha bármilyen jel mutat arra, hogy a jelszó kompromittálódhatott, azonnal meg kell változtatni és értesíteni kell az információbiztonsági felelőst;

e) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el.

A felhasználói jelszavak képzésénél az alábbi szempontokat kell betartani:

a) könnyen megjegyezhető, és nehezen kitalálható legyen;

b) semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja, ilyenek a nevek, telefonszámok, születési dátumok, stb.;

c) ne legyen a gépnévre vagy a felhasználói névre utaló;

d) ne legyen sorozat.

4.4. Regisztráció külső honlapokra

Külső honlapokra történő regisztrációt az adatgazdánál kell kezdeményezni az érintett munkatárs vezetőjének előzetes jóváhagyásával.

A jogosultságokról az érintett adatgazda nyilvántartást vezet a következő tartalommal:

- Honlap neve;
- Honlap leírása;
- Honlap adatgazdája;
- Honlap üzemeltetője;
- Felhasználó neve;
- Felhasználó szervezeti egysége;
- Felhasználó beosztása;
- Felhasználó azonosítója;
- Jogosultság kezdete;
- Jogosultság vége;
- Jogosultság leírása.

Változás esetén (felhasználói jogosultság visszavonása, módosítása) az érintett vezetőnek tájékoztatást kell adnia a rendszergazda részére, aki átvezeti azt a nyilvántartásban.

A külső honlapok jogosultságait - az érintett honlap adatgazdájának bevonásával - 2 évente felül kell vizsgálni és a szükséges módosításokat át kell vezetni a nyilvántartásba, illetve kezdeményezni kell azt az érintett honlap üzemeltetőjénél.

A felülvizsgálatot az IBF koordinálja.

4.5. Hozzáférés védelem mobil infokommunikációs eszköz esetén

A mobilitás miatt sokkal nagyobb veszélynek kitett mobil infokommunikációs eszközök esetében is jelszót kell használni a rendszerbe történő belépéshez. Bár ez a védelem megnehezíti

a hozzáférést, a háttértárolót eltávolítva az ott nyíltan tárolt adatok így is megszerezhetők. Ezek miatt a Hivatal titkosítja a mobil infokommunikációs eszközeinek háttértárolóit.

A fentiek miatt fokozottan kell törekedni ezen eszközök fizikai védelmére is az elvesztés, illetve ellopás ellen.

Külső munkahelyen történő feladat elvégzése után a keletkezett adatokat a hálózati meghajtóra kell menteni.

A mobil infokommunikációs eszközökről a feleslegessé vált adatokat le kell törölni.

Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát, az eszközhöz illetéktelenek ne férhessenek hozzá.

4.6. Adatmentések, az adathordozók nyilvántartása és tárolása

Az adatokat nem a helyi munkaállomáson, hanem a „Hivatali fájlszerver" megfelelő könyvtáraiban kell tárolni, ahol biztosított azok rendszeres mentése és biztonságos tárolása. Minden felhasználó számára rendelkezésre áll a „Saját" könyvtár a saját adatok tárolására, illetve minden iroda rendelkezik külön könyvtárral a szervezeti egységen belül keletkező és közösen kezelendő adatok tárolására. A nem megfelelő könyvtárba mentés a felhasználó felelőssége.

A Hivatal nem vállal felelősséget a helyi gépen tárolt adatokért.

A rendszergazda a „Hivatali fájlszerveren tárolt ügyviteli adatokról meghatározott módon és gyakorisággal mentést készít. Ebből adódóan lehetőség van az állományok, adattáblák statikus visszaállítására a mentés időpontjának megfelelő tartalommal. Folyamatok előre-, illetve visszagörgetésére a rendszer nincs felkészítve. Speciális mentési igényekről a rendszergazdát írásban értesíteni kell, és egyeztetni kell a kivitelezés lehetőségéről.

Az adat visszaállítást az adatgazda írásbeli (e-mail) igénye alapján a rendszergazda végzi el.

A feljegyzésnek tartalmaznia kell a visszaállítani kívánt adat:

a) utoljára ismert pontos helyét;

b) megnevezését, és a

c) visszaállítandó időpontot.

A felhasználónak a jogviszonyának megszűnésekor a munkaállomásán, a Hivatali tárhelyen, valamint az elektronikus információs rendszerekben kezelt és tárolt adatok törlése tilos!

4.7. Adathordozók kezelése

Az eszközhasználatot, a Hivatal elektronikus információs rendszereihez történő csatlakoztatása után, a Hivatal minden előzetes értesítés nélkül figyelheti, monitorozhatja.

A Hivatal informatikai infrastruktúrájából kivitt adatok biztonságát ebben az esetben is biztosítani kell a következő védelmi intézkedésekkel:

a) Otthoni számítógép esetén gondoskodni kell az operációs rendszer és az egyéb irodai alkalmazások naprakészségéről;

b) Az operációs rendszerbe épített helyi tűzfalat be kell kapcsolni;

c) Kémprogram elleni védekezéssel ellátott, naprakész vírusvédelemmel kell rendelkezni.

d) A napi munkavégzéshez használt felhasználói azonosítónak rendszergazda jog nem adható.

A Hivatal az informatikai rendszerében használt adathordozókat információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

5. FELHASZNÁLÓK SZÁMÍTÓGÉPES KÖRNYEZETE

5.1. Számítógépek és a hálózat kezelési előírásai

A felhasználó felelős az infokommunikációs eszközön általa végzett, nyilvánvalóan szakszerűtlen beavatkozásának következményeiért.

A felhasználó semmilyen infokommunikációs eszközt nem telepíthet a Hivatal elektronikus információs rendszerébe.

A Hivatal által biztosított infokommunikációs eszközök elhelyezését, telepítési módját nem változtathatja meg, azok borítását nem bonthatja meg, a konfigurációját nem módosíthatja. A Hivatal által biztosított infokommunikációs eszközökre szoftvert (ideértve a csak másolással telepíthető szoftvereket is) nem telepíthet, nem törölhet és nem módosíthat.

A felhasználónak infokommunikációs eszköz, illetve szoftver telepítési igényével a rendszergazdát kell megkeresnie. Az igénylést a munkahelyi vezetővel egyeztetve a Jegyző hagyja jóvá.

A rendszergazda bizonyos szoftver elemek telepítését Hivatali szétosztással, automatikusan végzi. Az ilyen távolról történő frissítéskor meg kell várni a frissítés befejeződését, a folyamatot leállítani tilos. El kell fogadni, hogy ez alatt az idő alatt a számítógép valamivel lassabban működik.

A Hivatal belső hálózatához idegen infokommunikációs eszköz nem csatlakoztatható.

5.2. Internethasználat, webböngészés

Az Internet és a webböngészés használatának főbb szabályai:

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja!

A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése), és adatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén a rendszergazda jelentést tesz az IBF-nek, aki eljár az ügyben a Jegyző felé.

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és Internet böngésző kontrollok is.

Tilos az IBF engedélye nélkül külső féllel nem web alapú hálózati kapcsolat kialakítása (pl.: FTP).

Tilos az elektronikus információs rendszerek használata a Hivatali értékekkel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes illetve szerencsejátékokra, bármilyen kereskedelmi, illetve jogellenes tevékenységre.

Tilos nem a munkavégzést szolgáló közösségi oldalak látogatása.

Tilos a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.

Főszabály szerint tilos Hivatali adatok felhő-alapú tárolása, illetve ezen adatok külföldi kezelése. Amennyiben felmerül a felhő-alapú és/vagy külföldi adatkezelés igénye, úgy a jelen IBSZ ***{Hiba! A hivatkozási forrás nem található.. Hiba! A hivatkozási forrás nem található.}*** jezetében foglaltak szerint kell eljárni.

Az internetről csak Hivatali célból lehet fájlokat letölteni! Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!

Az internetes oldalak elérése monitorozásra és naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

5.3. E-mail használat

A Hivatal által biztosított elektronikus levelezési cím és az elektronikus levelezési szolgáltatás kizárólag Hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos a Hivatali e-mail címüket nem hivatali minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra, az Interneten elérhető nyilvános chat-és fórum oldalakon Hivatali e-mail címmel hozzászólni stb.)!

A Hivatal által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata munkavégzésre nem engedélyezett.

Az e-mail a munkavégzéssel kapcsolatos levelezést szolgálja, ahol az egy felhasználóra eső tárterület korlátozott, és ennek túllépése esetén a rendszer figyelmeztetést küld, további figyelmeztetési határok átlépése esetén pedig megszűnhet a további levelezési lehetőség.

Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

A Hivatal elektronikus levelező rendszeréből elküldött elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására, mivel műszakilag - az elektronikus levelezési szolgáltatás működési elvéből fakadóan – a rendszergazdák nem tudnak garanciát vállalni arra, hogy az elektronikus levél

a) eljut a címzetthez;

b) átküldése közben illetéktelenek annak tartalmát el nem olvassák;

c) átküldése közben illetéktelenek annak tartalmát nem módosítják.

Amennyiben a fentiek biztosítására szükség van (pl.: elektronikus ügyintézés), akkor az állam által nyújtott Hivatali Elektronikus Ügyintézési Szolgáltatásokat kell igénybe venni vagy egyéb kriptográfiai algoritmusokat kell alkalmazni az elküldött elektronikus levelek bizalmasságának és sértetlenségének biztosítása érdekében.

A fentiekhez hasonlóan a rendszergazdák arra sem tudnak garanciát vállalni, hogy egy Hivatali címzettnek szóló levél időben és sértetlenül megérkezik a címzetthez, mivel ehhez más, külső szolgáltatók közreműködése is szükséges, illetve a Hivatal a tömeges, kéretlen, valamint kártékony levelek elleni védekezésül spamszűrő rendszert működtet, mely kivételes esetben (fals pozitív) kiszűrhet hasznos levelet is.

A Hivatal elektronikus levelező rendszeréből csak akkor lehet bizalmas, jogszabály által védett adatot, titkot (személyes adatok, különleges adatok, adótitok stb.) elküldeni, hogy ha szabványos, sérülékenységektől mentes kriptográfiai algoritmussal az adat titkosításra került.

A felhasználók alapértelmezésben a levelezés során csak a saját postaládájukat tudják kezelni, mások postaládáit nem látják.

Más felhasználó postafiókjához történő hozzáférést csak a Jegyző engedélyezhet, ebben az esetben a teljes igénylési folyamatot a vonatkozó űrlap kitöltésével dokumentálni szükséges.

A felhasználónak tilos a postafiókjában kezelt elektronikus levelek automatikus vagy manuális továbbítása más, külső elektronikus levelező rendszerbe (pl.: a saját magán e-mail címére).

Zavaró, félreinformáló levelek, spamek küldése, jogtalan megrendelések elindítása tilos, és eljárást vonhat maga után.

Ismeretlen helyről származó e-mailek, illetve azok csatolmányainak megnyitásakor és az azokban elhelyezett hivatkozásokra kattintással fokozott óvatossággal kell eljárni, mert maga az e-mail vagy annak csatolmánya, illetve az e-mailben elhelyezett hivatkozás kártékony lehet. Ebben az esetben ellenőrizni kell az e-mail feladóját, a tárgyat, a levél szövegezését (magyartalan megfogalmazás), a szükségtelen csatolmányokat és a levélben elhelyezett hivatkozásokat.

6. VÍRUSVÉDELEM

6.1. A vírusvédelem alkalmazásának előírásai

A rendszergazda a számítógépek vírusok elleni védelmére rendszeresen frissített vírusvédelmi rendszert, és anti-spyware programot üzemeltet. Ez a védelem kiterjed a kiszolgálók, munkaállomások, valamint a teljes Internet és elektronikus levélforgalom folyamatos ellenőrzésére. Új vírus megjelenése esetén még így is előfordulhat fertőzés, valamint csatolmányok, CD és DVD lemezek, cserélhető adathordozók, illetve internetről letöltött fájlok használata esetében.

Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.

Dokumentumok esetében lehetőség szerint kerülni kell a makrók megnyitását, külső forrásból érkező dokumentumok esetében pedig nem szabad engedélyezni.

Ha a vírus helye nem lokalizálható, a rendszergazda jogosult a hálózat egyes funkcióit, vagy a teljes hálózat felhasználói szolgáltatásait a vírusveszély elhárításáig felfüggeszteni.

6.2. Teendők vírusgyanú esetén

Vírusgyanú esetén a felhasználó köteles azonnal felhívni a rendszergazdát, aki ellátja utasítással, vagy intézkednek a jelzés továbbításáról az információbiztonsági felelős felé.

7. AZ INFORMATIKAI ESZKÖZÖK FIZIKAI VÉDELME

7.1. Számítógép használatának előírásai

A munkaállomást és a perifériákat a napi munkavégzés befejezésekor ki kell kapcsolni. Ez alól kivételek azok az eszközök, amelyek automatikusan kikapcsolnak (hálózati nyomtatók vagy a modern monitorok többsége stb.). Az infokommunikációs eszközöket üzem közben letakarni, a szellőző nyílásokat eltakarni tilos!

7.2. „Üres asztal - tiszta képernyő" politika

Az „üres asztal - tiszta képernyő" politika megvalósítása az alábbiakat jelenti:

a) A monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);

b) A felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;

c) A munkavégzés befejeztével a munkaállomásból ki kell jelentkezni, illetve ki kell azt kapcsolni;

d) Elfelejtés esetére jelszóvédett, automatikus zárolás kerül beállításra, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

e) A felhasználóknak az infokommunikációs eszközök elhelyezésére szolgáló helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik;

f) A kinyomtatott, faxolt vagy másolt iratokat nem szabad őrizetlenül a nyomtatókban, multifunkcionális eszközökben, fax-okban hagyni.

g) Ügyfelet és más külső felet nem szabad felügyelet nélkül az irodában hagyni.

7.3. Mobil infokommunikációs eszközök védelme

A munkaállomásokra vonatkozó előírásokon kívül az alábbi védelmi szabályokat kell betartani:

a) mechanikai és használati sérülések elkerülése érdekében követni kell a géphez kapott használati útmutatót;

b) cserélhető kártyák behelyezésénél, és eltávolításánál szintén a használati utasítást kell követni;

c) a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek. Gondoljunk erre, és ne hagyjuk őrizetlenül autóban, szállodai szobában stb. (zárjuk el fizikailag, használjuk, ha lehet az értékmegőrzőt, ha nincsenek érzékeny adatok a gépen);

7.3.1. Mobil infokommunikációs eszközök ellopása

A mobil infokommunikációs eszközök ellopása esetén:

a) az ellopás tényét a lehető leggyorsabban jelenteni kell az információbiztonsági felelősnek és a munkahelyi vezetőnek;

b) értesíteni kell a rendőrséget;

c) értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;

d) valamennyi rendőrségi jelentést meg kell őrizni és a Hivatal részére át kell adni.

7.3.2. Infokommunikációs eszköz elvesztése

Bármely infokommunikációs eszköz eltűnését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek és az információbiztonsági felelősnek és tájékoztatni kell őket arról, hogy a berendezés tartalmaz-e bárminemű érzékeny információt. (Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve.)

8. INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK KEZELÉSE

Információbiztonsági eseménynek minősül minden 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, így különösen

a) a szolgáltatás, a berendezés vagy az eszközök elvesztése;

b) a rendszer hibás működése vagy túlterhelések (DoS-támadás);

c) emberi hibák;

d) a szabályzatoknak vagy irányelveknek való nem megfelelés;

e) a fizikai biztonsági rendelkezések megsértése;

f) nem ellenőrzött rendszerbeli változások;

g) a szoftver vagy hardver hibás működése;

h) hozzáférési előírások megsértése;

i) kártékony kód általi fertőzés;

j) a nem teljes vagy nem pontos működési adatokból eredő hibák;

k) a bizalmasság és sértetlenség megsértése;

l) az elektronikus információs rendszerrel való visszaélés.

8.1. Jelentés a biztonsági eseményekről

A biztonságot érintő eseményekről a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és a rendszergazdát. A rendszergazda értesíti az információbiztonsági felelőst, aki jogosult az esemény kivizsgálására.

A biztonságot érintő eseményekről szóló jelentések elkészítésére az IBSZ *{5. számú melléklet – Biztonsági események jelentése}* mellékletét kell használni.

8.2. Jelentés a szoftverzavarokról

Az elektronikus információs rendszerekben tapasztalt szoftverzavarokat jelenteni kell a rendszergazdának. Szoftverzavarra utaló jelek lehetnek, amikor az alkalmazás nem a várt eredményt adja vagy nem a megszokott képernyőképek jelennek meg.

A jelentéshez az IBSZ *{5. számú melléklet – Biztonsági események jelentése}* mellékletét kell használni. Szoftverzavarok esetén legalább a következő feladatokat végre kell hajtani:

a) fel kell jegyezni a zavaró jelenséget és a képernyőn megjelenő minden üzenetet és

b) be kell szüntetni az adott számítógép használatát.

A felhasználóknak tilos a hibásnak feltételezett szoftvert eltávolítaniuk az elektronikus információs rendszerből, illetve kísérletet tenni a hiba elhárítására.

A hibaelhárítást és helyreállítást a rendszergazda hajthatja végre.

Abban az esetben, ha feltételezhető az információbiztonság sérülése, akkor az eseményt a rendszergazdának jelentenie kell az információbiztonsági felelősnek, aki kivizsgálja az eseményt.

5. számú melléklet – Biztonsági események jelentése

A biztonsági esemény megnevezése:

A tapasztalás helye és időpontja:

Az érintett személyek megnevezése:

Az esemény pontos leírása:

Az észlelő neve:

Dátum:_____év___hó___nap …… ……

Észlelő aláírása IBF aláírása

Az esemény kivizsgálásának leírása:

Tett intézkedés leírása:

Az intézkedés életbelépésének időpontja:

Végleges-e az intézkedés:

☐	*Igen*
☐	*Nem*

Igényel-e kockázatelemzést az esemény:

☐	*Igen*
☐	*Nem*

Dátum:_____év___hó___nap …… ……

Információbiztonsági felelős aláírása Jegyző aláírása

6. számú melléklet – Felhasználói Nyilatkozat

Nyilatkozat

Alulírott (név: ,.....
beosztás:.....
szervezeti egység: .....),
kijelentem, hogy a Sárbogárdi Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának és/vagy Felhasználói Informatikai Biztonsági Házirendjének tartalmát megismertem és elfogadom, hogy azt munkám során betartom, illetve betartatom (vezetők esetén).

Kelt: ……

Aláírás

7. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

Információbiztonsági tájékoztatás

1. Tájékoztatom, hogy a Sárbogárdi Polgármesteri Hivatallal (továbbiakban: a Hivatal) fennálló jogviszonya megszűnésének napjától, ……..-től a Hivatal elektronikus információs rendszereihez való hozzáférési jogosultsága megszűnt. Legkésőbb ezen a napon köteles a használatában lévő, a Hivatal elektronikus információs rendszerével kapcsolatos valamennyi eszközt hiánytalanul, sértetlenül munkáltatója részére visszaszolgáltatni.
2. A Hivatalnál működő elektronikus információs rendszereket a Hivatal kizárólag Hivatali munkavégzés céljából biztosítja a munkatársak részére, az elektronikus információs rendszerekben keletkező és ott tárolt, kezelt adatok, információk vonatkozásában a Hivatal fenntartja magának a tulajdonjogot.
3. A Hivatalnak továbbra is hozzáférési lehetősége van az Ön által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.
4. Jogviszonyának megszűnését követően nem jogosult a Hivatal elektronikus információs rendszereiben tárolt, jogviszonya folytán készített, illetve megismert adatokat felhasználni, azokat további személyek tudomására hozni, valamint a megismert és használt elektronikus információs rendszerek összetételéről, felépítéséről, működéséről további személyek számára bárminemű információt közölni.
5. A 4-es pontban megfogalmazott jogellenes magatartásnak polgári- és büntetőjogi következményei lehetnek.

Kelt: ……

……

Jegyző

A fenti tájékoztatást tudomásul vettem:

Kelt: ……

……

munkavállaló neve

…….

aláírása

8. számú melléklet – Titoktartási Nyilatkozat

TITOKTARTÁSI NYILATKOZAT

Alulírott

Név: .....

Anyja neve: .....

Lakcím: .....

Sz. ig. szám: .....

a ..... munkatársa kijelentem, hogy

a Sárbogárdi Polgármesteri Hivatal**,** mint **Megrendelő**,

valamint .....

mint **Vállalkozó**

között

.....tárgyú,

..... **-én megkötött vállalkozási/megbízási/szállítási szerződés**

keretében elvégzett feladatok során tudomásomra jutott információkat és adatokat bizalmasan kezelem és megtartom. A tudomásomra jutott információkat, adatokat az érdekkörön kívüli személlyel nem közlöm. Ezen felelősségem fennáll azt követően is, ha a

..... -vel való szerződéses jogviszonyom bármely okból megszűnik.

Kelt: ……

……

Nyilatkozó

	Tanú 1	**Tanú 2**
Aláírás:	.....	.....
Neve:	.....	.....
Anyja neve:	.....	.....
Lakcím:	.....	.....
Sz. ig. szám:	.....	.....