ESZTERHÁZY KÁROLY FŐISKOLA

INFORMATIKAI BIZTONSÁGI POLITIKA

(Elfogadva a Szenátus a 81/2009. (XI.4.) számú határozatával)

Eger, 2009.

ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályozás tárgya, alkalmazási területe

Ez a dokumentum meghatározza az Eszterházy Károly Főiskola (a továbbiakban: Főiskola) informatikai rendszereiben előállított, tárolt, használt és továbbított információk elégséges biztonságának megteremtéséhez szükséges illetve ajánlott intézkedéseket.

Azoknak ad segítséget az informatikai biztonság szervezeti szintű kezeléséhez, akik a Főiskolán a biztonság kezdeményezéséért, megvalósításáért és megtartásáért felelnek.

2. Az Informatikai Biztonsági Politika célja

Az Informatikai Biztonsági Politika (a továbbiakban: IBP) célja a Főiskola informatikai rendszerei által kezelt adatok és információk *bizalmasságának, hitelességének, teljességének, sértetlenségének és rendelkezésre állásának* (összefoglaló szóval: biztonságának) biztosítása, ezen belül különösen a következők:

- Irányelvek meghatározása az informatikai biztonsági feladatok összehangolt, tervszerű végrehajtásának biztosítása érdekében.
- A informatikai rendszereket működtető IK és a főiskolai szervezeti egységek informatikai biztonsággal kapcsolatos felelősségi köreinek elhatárolása, az együttműködés módjának rögzítése.
- Útmutatás az érintett vezetőknek az informatikai biztonságot érintő döntések meghozatalához.
- Egységes IT biztonság követelmények meghatározása, ide értve a külső felekkel szembeni elvárásokat is.
- Az informatikai biztonsággal kapcsolatos jogszabályi kötelezettségeknek és ajánlásoknak való megfelelés minél teljesebb körű biztosítása.

Célja egységes elveken nyugvó, a nemzetközi és hazai szabványokhoz, ajánlásokhoz igazodó olyan előírások biztosítása az informatikai biztonság megteremtéséhez, amelyek bizalmat teremthetnek az informatikai rendszer biztonságát illetően.

3. Az Informatikai Biztonsági Politika hatálya

„Az Informatikai Biztonsági Politika célja” fejezetben meghatározott célok megvalósítása érdekében jelen dokumentum előírásai és ajánlásai az alábbiakban felsorolt területekre terjednek ki.

3.1. *Tárgyi hatály*

Az IBP hatálya kiterjed a következőkre:

- a Főiskola bármely szervezeti egysége által használt (fejlesztett, vásárolt vagy bérelt) illetve üzemeltetett, továbbá a Főiskola tulajdonában lévő informatikai eszköz és berendezés, amely tárolja, kezeli, feldolgozza, felügyeli, ellenőrzi és/vagy továbbítja a Főiskola tulajdonában/kezelésében lévő adatokat, információkat;
- a Főiskola területén bármely okból használt, más személy vagy szervezet tulajdonát képező informatikai eszköz és berendezés;
- a fenti kategóriák valamelyikébe tartozó informatikai eszközökön használt vagy tárolt szoftverek és adatok (rendszerprogramok, alkalmazások, adatbá-

zisok, stb.), ideértve az üzemelő rendszerek adatain kívül az oktatási, teszt és egyéb célra használt adatokat is;

- az informatikai területen használt összes dokumentáció (szervezési, fejlesztési, programozási, üzemeltetési, stb. dokumentumok), függetlenül azok formátumától és az adathordozótól (elektronikus, papír, stb.).
- a Főiskola által kezelt, elektronikus adathordozón tárolt adatok teljes köre, felmerülésüktől, feldolgozási és tárolási helyüktől függetlenül.

3.2. *Területi hatály*

Az IBP hatálya kiterjed a Főiskola székhelyére, minden telephelyére, továbbá mindazon objektumokra és helyiségekre, amelyekben a „Tárgyi hatály" pontban meghatározott eszközöket, szoftvereket, adatokat vagy dokumentumokat hoznak létre, tárolnak, felhasználnak, vagy továbbítanak.

3.3. *Személyi-szervezeti hatály*

Az IBP hatálya kiterjed mindazon személyekre, akik munkájuk végzése során vagy egyéb céllal a „Tárgyi hatály" pontban meghatározott eszközöket, szoftvereket, adatokat vagy dokumentumokat hoznak létre, tárolnak, felhasználnak, vagy továbbítanak, illetve azokra, akik ezen tevékenységekkel kapcsolatosan döntéseket hoznak. Ezen személyek körébe tartoznak a Főiskolánál foglalkoztatott munkavállalók, továbbá az informatikai rendszerrel kapcsolatba kerülő, de nem a Főiskola alkalmazásában álló természetes és jogi személyek is.

3.4. *Időbeli hatály*

Az IBP a hatályba lépés napjától a visszavonásig érvényes.

3.5. *További hatály*

Az IBP hatálya kiterjed a fenti pontokban felsorolt területekkel kapcsolatos szabályozásokra és utasításokra. Ennek megfelelően az IBP-vel ellentétes szabályozás illetve utasítás a Főiskolán nem léphet hatályba.

4. Informatikai biztonságpolitikai alapelvek

Az informatikai biztonsági kérdések tekintetében a bizalmasság, sértetlenség és rendelkezésre állás alapelveit kell érvényesíteni.

A Főiskola feladatait figyelembe véve az általános érvényű informatikai biztonsági alapelveket (lásd: 1. sz. melléklet) a következőképpen kell értelmezni:

a. **bizalmasság**: biztosítani kell a megfelelő védelmet a Főiskola kezelésében és használatában lévő adatok és információk tekintetében mind a központi, mind a helyi feldolgozások és az adat- és információcsere során;

b. **sértetlenség**: biztosítani kell a Főiskola által kezelt, feldolgozott és közzétett adatok folyamatos pontosságát és teljességét mind a feldolgozás, mind pedig az adat- és információcsere során;

c. **rendelkezésre állás**: biztosítani kell a külső és belső adatkérések során a jogosultak számára a folyamatos hozzáférhetőséget.

5. Védelmi célkitűzések, biztonsági követelmények

5.1. A Főiskola informatikai biztonságának megteremtése érdekében az alábbiakról kell gondoskodni:

a. az informatikai biztonság részletes követelményeinek rögzítése az informatikai biztonsági dokumentációs rendszerben;

b. az informatikai biztonsággal kapcsolatos szervezeti és hatásköri kérdések, valamint a Főiskolán belüli és az azon kívüli adatkapcsolatok szabályozása;

c. a Főiskola adat és információs vagyonának védelmét szolgáló minősítési és biztonsági osztályba sorolási eljárás kialakítása, valamint annak ellenőrzési módja;

d. a személyekhez és szerepkörökhöz kapcsolódó biztonsági követelmények, az oktatási és képzési tervek, valamint biztonsági események és meghibásodások esetén szükséges eljárások kialakítása;

e. az informatikai biztonsághoz kapcsolódóan az informatikai rendszerek fizikai és környezeti biztonságának kialakítása;

f. az alkalmazott üzemeltetési és kommunikációs eljárások informatikai biztonsági követelményrendszerének meghatározása;

g. az informatikai eszközökhöz, adatokhoz és informatikai szolgáltatásokhoz történő hozzáférés szabályainak kialakítása és alkalmazása;

h. az informatikai rendszerfejlesztési és karbantartási eljárások létrehozása;

i. az informatikai infrastruktúra folyamatos működésének biztosítását szolgáló eljárások kialakítása;

j. az informatikai infrastruktúra, eljárások és szolgáltatások törvényi és jogszabályi megfelelőségét biztosító szabályozás kialakítása.

5. 2. A védelmi célkitűzések és informatikai biztonsági követelmények teljesítése érdekében biztosítani kell a kellő, ésszerű, költség-hatékony, kockázatokkal arányos védelmi intézkedések és kontrollok – a mindenkori rendelkezésre álló erőforrásoknak megfelelő – alkalmazását.

6. Az Informatikai Biztonsági Politika érvényesítése

Az Informatikai Biztonsági Politika irányelveinek megvalósulása és érvényre juttatása céljából:

a. az utasítás hatálya alá tartozó személyek kötelesek az informatikai biztonságpolitikai alapelvek és az informatikai biztonsági dokumentációs rendszer egyéb előírásainak megfelelően eljárni;

b. kötelesek továbbá megőrizni a Főiskola informatikai szolgáltatásainak minőségét, jó hírét, szellemi és vagyoni értékeit, illetve a vonatkozó hatályos törvények, jogszabályok és belső utasítások által előírt információ- és adatkezelésre vonatkozó követelményeket betartani;

c. az utasítás hatálya alá tartozó természetes vagy jogi személyek felelősségére vonatkozó szabályokat a velük kötött (munka)szerződéseknek kell tartalmazniuk.

Az informatikai biztonság szabályozási rendszerének egyik alapvető eszköze a biztonsággal kapcsolatos szerepkörök szétválasztása annak érdekében, hogy megakadályozza a felelős tevékenységek és az ellenőrzésükhöz szükséges jogosultságok összeférhetetlen alkalmazását.

7. Vonatkozó jogszabályok, belső szabályozás, szabványok és ajánlások

7.1. Jogszabályok

- 184/2004. (VI. 3.) Korm. rendelet az elektronikus közigazgatási ügyintézésről és a kapcsolódó szolgáltatásokról;
- 84/2007. (IV. 25.) Korm. rendelet a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről;
- 2005. évi XC. Trv. Az elektronikus információszabadságról;
- 305/2005. (XII. 25.) Korm. rendelet a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzés adattartalmára, az adatintegrációra vonatkozó részletes szabályokról.

7.2. A Főiskola kapcsolódó belső utasításai

- Szervezeti és Működési Szabályzat
- Informatikai Stratégia
- Iratkezelési Szabályzat
- Tűzvédelmi Szabályzat

7.3. Nemzetközi és hazai szabványok, ajánlások

- ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements (magyarul MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények) szabvány
- ISACA:2005 Control Objectives for Information and Related Technology (COBIT), http://www.isaca.org/cobit
- A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonság Ajánlások (2008)
- A Kormányzati Informatikai Egyeztető Tárcaközi Bizottság 23. számú ajánlása: Az informatikai szerződések általános követelményei (2005)

8. Az Informatikai Biztonsági Politika életciklusa

8.1. A Főiskola IBP-je naprakészen tartást és rendszeres felülvizsgálatot, és aktualizálást igényel, ezért

a. éves rendszerességgel ellenőrizni kell az IBP-t, tekintettel a legutolsó ellenőrzés óta bekövetkezett szervezeti, jogszabályi, funkcionális, személyi, biztonsági, technológiai vagy egyéb változásokra;

b. az IBP karbantartásának kezdeményezése és módosítási javaslatok készítése az Informatikai Biztonság Felügyelő feladata;

c. szükség esetén az összegyűjtött módosítási javaslatok mérlegelése és elfogadása céljából Informatikai Biztonsági Stratégiai Fórum hívható össze az Informatikai Bizottság részeként.

8.2. A módosított IBP-t minden esetben a Főiskola vezetőjének kell jóváhagyásra előterjeszteni.

8.3. Rendkívüli felülvizsgálat a következő esetekben rendelhető el, ha:

a. új munkafolyamatok, szervezeti egységek, szolgáltatások jelennek vagy szűnnek meg;

b. új informatikai technológiák kerülnek bevezetésre vagy szűnnek meg;

c. a kockázatelemzés következtében új, lényeges kockázatok válnak ismertté;

d. olyan súlyos informatikai biztonsági események („incidensek") bekövetkezésekor, amelyek érzékeny vagy minősített adatokat, információkat érintenek;

e. a Főiskola igényei, céljai megváltoznak;

f. bármilyen más okból az IBP nem tölti be szándékolt szerepét.

8.4. Lényeges módosítás esetén megfelelő türelmi időt szükséges hagyni az új IBP irányelvek kihirdetése és azok érvényességi kezdete között annak érdekében, hogy az érintettek fel tudjanak készülni a változásra.

AZ INFORMATIKAI BIZTONSÁGI IRÁNYÍTÁSI RENDSZER

1. fejezet

Az Informatikai Biztonsági Irányítási Rendszer (IBIR)[1] egy általános irányítási rendszer, amely az üzleti kockázat elemzésén alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot.

1.1. A Főiskola informatikai biztonságának megteremtése és folyamatos fenntartása érdekében

a. Informatikai Biztonsági Irányítási Rendszert kell kialakítani;

b. informatikai biztonsági eszközöket kell alkalmazni;

c. informatikai biztonsági oktatásokat és képzéseket kell szervezni;

d. a szabályzatokban előírtak betartását ellenőrizni kell;

e. évenként informatikai biztonsági vizsgálatokat kell tartani.

1.2. A Főiskola informatikai biztonságával kapcsolatos elvárásokat, szabályokat és folyamatokat az Informatikai Biztonsági Dokumentációs Rendszerben (IBDR) kell rögzíteni.

Az IBDR az alábbi szerkezet szerint épül fel:

Informatikai
Biztonsági
Politika

Informatikai Biztonsági Szabályzat

[1] Information Security Management System (ISMS) – az ISO/IEC 27001:2005 szabvány alapvető fogalma.

Katasztrófa-elhárítási terv	Alsóbbrendű szabályozások	Felhasználói kézikönyvek

1.3. Az informatikai biztonsági rendszer dokumentumai

A Főiskola – a működését támogató információrendszerére vonatkozóan – a 3.-12. fejezetekben felsorolt területek részletes szabályozása révén biztosítja az informatikai biztonságot.

a. Az Informatikai Biztonság Politika: jelen dokumentum, amely meghatározza az informatikai infrastruktúra teljes életciklusára (tervezés, bevezetés, fejlesztés, üzemeltetés és selejtezés) alkalmazandó általános biztonsági *elvárásokat*.

b. Az Informatikai Biztonság Szabályzat (IBSZ): részletesen meghatározza az IBP által előírt, a biztonság általános és speciális követelményeit megvalósító *intézkedéseket (kontrollokat)*, azok dokumentálásának, ellenőrzésének feladatait, felelőseit és a végrehajtás gyakoriságát és idejét.[2]

c. Katasztrófa-elhárítási terv: az informatikai vészhelyzetek elhárítására ad forgatókönyvet, amikor az erőforrások átfogó sérülése miatt a rendszerek folyamatos és rendeltetésszerű működése megszakad.

d. Alsóbbrendű szabályozások (végrehajtási eljárásrendek): a műszaki berendezések kezelési szabályai, kiemelt folyamatok végrehajtásának, ellenőrzésének módja, folyamata (pl. mentési szabályzat, üzemeltetői és adminisztrátori dokumentumok, műszaki specifikációk, vírusvédelem, konfigurációk kezelésének rendje, stb.) az IBP követelményei és az IBSZ alapján kerülnek alkalmazásra.

e. Felhasználói kézikönyvek.

1.4. A dokumentációs rendszer felülvizsgálata és értékelése

a. Az IBDR aktualitásának fenntartása érdekében a rendszerben található dokumentumok mindegyikében rendszeres felülvizsgálati és karbantartási eljárást kell definiálni, amely rögzíti az eljárással kapcsolatos feladatokat, kötelességeket.

b. A dokumentációs rendszer részeit rendkívüli felülvizsgálat alá kell vonni az „ÁLTALÁNOS RENDELKEZÉSEK 8. Az Informatikai Biztonsági Politika életciklusa” c. fejezetében meghatározott események teljesülése esetén.

[2] Az IBSZ-nak tartalmaznia kell mindazokat az eljárásokban alkalmazott követelményeket, amelyeket a Főiskola az informatikai biztonsággal kapcsolatban megfogalmaz, és amelyeket minden, az IBP hatálya alá tartozó személynek és szervezetnek be kell tartania.

AZ IBIR BEVEZETÉSE ELŐTT ELVÉGZENDŐ FELADATOK

2. fejezet

a. Fel kell mérni és meg kell ismerni a főiskolán jelenleg uralkodó *információbiztonsági kultúrát*, az alkalmazott kontrollokat, azok működési hatékonyságát.

b. Fel kell mérni az *informatikai irányítás* jelenleg szintjét.

c. *Informatikai vagyonleltárt* kell készíteni.

d. Ki kell alakítani a *vagyonelemeket érintő kockázatok* felmérésének, elemzésének és kezelésének módszerét.

e. *Alkalmazhatósági nyilatkozatot* kell kiadni.

f. Ki kell alakítani a *szabályozási környezetet*.

g. *Dokumentációs rendszert* kell kialakítani.

h. Biztosítani kell *a vezetés elkötelezettségét*.

i. Meg kell határozni a főiskola értékei védelmének és a biztonsági folyamatok *felelőseit*.

j. Biztosítani kell a megfelelő *erőforrásokat* az informatikai biztonsági követelmények megvalósításához.

AZ INFORMATIKAI BIZTONSÁG SZERVEZETE

3. fejezet

Az információbiztonság a főiskolai szervezet működési kultúrájának szerves része kell, hogy legyen. Az informatikai biztonság megfelelősége és annak megvalósításával kapcsolatos feladatok ellátása részben az üzemeltető, részben a vezetés, részben a felhasználók felelőssége.

3.1. Az informatikai biztonság felelős szerepkörei(nek kiosztása)

3.1.1. A Főiskola szervezetén belül az alábbi speciális feladatkörök biztosítják az elégséges biztonság megteremtését:

- a *Informatikai Központ (IK, a továbbiakban: Üzemeltető) vezetője*, aki összehangolja és irányítja az Üzemeltető által nyújtott informatikai szolgáltatások tervezését, a szolgáltatásnyújtáshoz szükséges folyamatok kialakítását és ellenőrzését;
- az *Informatikai Biztonsági Felügyelő*, akinek a feladata az informatikai biztonsággal kapcsolatos részletes követelmények meghatározása, a biztonsági követelmények teljesülésének felügyelete és ellenőrzése, valamint az informatikai biztonság megsértését eredményező valós vagy feltételezett események kivizsgálása.

A Főiskola rektora dönt ezeknek a feladatoknak és felelősségeknek a Főiskola szervezetén belüli megosztásáról, és ő jelöli ki a kapcsolódó szerepköröket betöltő személyeket is.

Az Informatikai Biztonsági Felügyelő szerepkörét el kell különíteni az informatikai rendszerek mindennapos üzemeltetési feladatoktól;

3.1.2. Az intézményen belül az informatikai biztonsági tevékenységek ellátása és felügyelete a IK feladata.

A IK vezetőjének a feladata meghatározni a belső, és a külső szervezetekkel történő elektronikus kommunikáció és adatcserék informatikai biztonsági követelményeit.

Minden olyan esetben, amikor az informatikai biztonság alapelvek, és célkitűzések érvényre juttatásához szükséges döntés meghaladja az informatikai vezető illetékességét és hatáskörét, *Informatikai Biztonsági Stratégiai Fórum* hívható össze az Informatikai (Stratégiai) Bizottság keretén belül. A Fórumot a IK vezetője hívja össze.

A Főiskola igénybe vehet külső informatikai biztonsági szakértőket annak érdekében, hogy alkalmas, független szakértelem álljon rendelkezésre az informatikai biztonsági kérdésekben vagy a biztonsági események kivizsgálása és értékelése céljából. A szakértők dolga, hogy gondoskodjanak a különböző szabványok és ajánlások alkalmazásáról.

3.1.3. Az informatikai biztonsággal kapcsolatos egyéb felelősségek:

- *Informatikai Biztonsági Felelősök*: akik általában – de nem szükségszerűen – a rendszergazdai feladatokat ellátó munkatársak közül kerülnek ki és az IT biztonsággal kapcsolatos üzemeltetési jellegű feladatokat látják el;
- *Adatgazda*: olyan intézkedési, döntési jogkörrel rendelkező vezető, aki egy meghatározott adatcsoport tekintetében az adatok fogadásában, tárolásában, feldolgozásában vagy továbbításában érintett szervezeti egységet képvisel, és az adott adatcsoport felhasználásának kérdéseiben (például felhasználói jogosultságok engedélyezése és megvonása) elsődleges döntési jogkörrel rendelkezik;
- *Felhasználó*: olyan személy, aki az IBP irányelvek hatálya alá tartozó informatikai rendszereket vagy eszközöket jogszerűen, megfelelő felhatalmazás alapján használja.

3.1.4. Biztonsági eseményekre és meghibásodásokra való reagálás

Az informatikai biztonsági események eredményes és hatékony kezelésének feltétele, hogy az informatikai biztonságért felelős vezetés mielőbb értesüljön a bekövetkezett biztonsági esemény(ek)ről. Ennek érdekében ki kell alakítani egy formális eljárásrendet, hogy a felhasználók jelenteni tudják a biztonsági eseményeket.

Minden alkalmazottnak fel kell tudnia ismernie – a saját tevékenysége körében – a különböző informatikai biztonsági eseményeket (pl. biztonsági rések, fenyegetések, gyenge pontok, meghibásodások). A felhasználónak a lehető legrövidebb időn belül jelentenie kell az észlelt vagy vélt biztonsági eseményt a közvetlen munkahelyi vezetőjének vagy az Informatikai Biztonsági Felügyelőnek.

3.2. Külső szolgáltatók igénybevétele (kiszervezés)

A Főiskola egyes informatikai feladatok – időszakos vagy folyamatos végrehajtására – külső feleket (cégeket, szakértőket) vehet igénybe. Az informatikai feladatok kiszervezése estén a külső féllel szerződést kötő fél felelős:

- a külső fél bevonása által okozott informatikai biztonság kockázatok felméréséért és értékeléséért;

- az informatikai biztonsággal kapcsolatos követelmények meghatározásáért, kommunikálásáért és a vonatkozó szolgáltatási megállapodásokba, szerződésekbe történő beépítéséért;
- a külső szerződő féllel történő megállapodást úgy kell megkötni, hogy az a lehető legkisebb kockázatot jelentse a Főiskola számára;
- a szerződés során különös figyelmet kell fordítani a biztonsági folyamatokra és ellenőrzésükre, a hálózatokhoz és munkaállomásokhoz történő hozzáférésre;
- a vonatkozó jogszabályok és belső szabályzatok átadásáért és megismertetéséért;
- az informatikai biztonsági követelmények, jogszabályok és szabályzatok betartásának ellenőrzéséért, szükség esetén a megfelelő szankcionálásért.

A meglévő megállapodásokat, szerződéseket legalább évenként felül kell vizsgálni, és a szükséges módosításokat el kell végezni.

3.3. Harmadik féllel kapcsolatos biztonság

Adott esetekben Főiskolának szüksége van szakértőkre, külső partnerekre, akiknek az intézmény érdekében végzett munkájuk során hozzáférést kell biztosítani a Főiskola adataihoz, informatikai rendszereihez.

A harmadik féllel való kapcsolatok biztonsága érdekében, meg kell határozni:

- a Harmadik féllel való kapcsolatok kockázatait és azok kezelését;
- az intézmény adataihoz, informatikai rendszereihez való hozzáférésre vonatkozó biztonsági és ellenőrzési követelményeket.

INFORMATIKAI VAGYONTÁRGYAK KEZELÉSE

4. fejezet

Annak érdekében, hogy az *intézményi információs vagyon* (meta-, feldolgozott és üzemeltetési adatok, információk) bizalmasságának megfelelően differenciált védelmi intézkedések kerüljenek kialakításra, szükséges az információs vagyontárgyak tulajdonosi felelősségének meghatározása, továbbá adatvédelmi és biztonsági súlyuknak megfelelő osztályozásuk.

4.1. Felelősség az informatikai vagyontárgyakért

Az információs vagyon rendelkezésre állása és megfelelő védelme érdekében minden fontos információs vagyontárgyat (materiális és immateriális eszközt egyaránt, mind az elektronikus, mind a papír hordozójút) kijelölt *tulajdonoshoz* kell rendelni, és meg kell határozni, hogy ki és milyen módon viseli a felelősséget a vagyontárgyért.

Az informatikai vagyontárgyakat nyilvántartásba kell venni a következő csoportosítás szerint:

- adatok
- alkalmazások
- informatikai infrastruktúra (pl. hardverek, szoftverek, stb.)

A vagyontárgyak azonosításához szükséges adatokat a nyilvántartásban kell rögzíteni, biztonsági osztályba kell sorolni, és meg kell nevezni a vagyontárgy felelősét. Ezt a nyilvántartást az informatikai területnek és a gazdálkodási területnek is naprakészen kell vezetnie, a két nyilvántartás egyezése érdekében folyamatosan ellenőrizni kell azokat.

4.2. Az informatikai rendszerben kezelt adatok biztonsági osztályokba sorolása

Az informatikai rendszerekben kezelt adatokat, információkat (és magukat a rendszereket is) megfelelő információvédelmi kategóriák szerint kell csoportosítani (biztonsági osztályokba sorolás).

Az alkalmazott többszintű, biztonsági osztályba sorolási modellt mindenkor a hatályos titokvédelmi törvény, az EU ajánlások, valamint az informatikai biztonsági iparági ajánlások alapján kell kialakítani.

Az intézmény birtokában és/vagy kezelésében lévő adatok, információk biztonsági osztályba sorolási rendjét részletesen az IBSZ tartalmazza.

A biztonsági osztályokba sorolást minden, a Főiskola bármely szervezeti egysége által tárolt vagy feldolgozott adatcsoport tekintetében el kell végezni. Amennyiben a kezelt adatok köre bővül, az osztályozást az új adatcsoportokra is végre kell hajtani.

A biztonsági osztályba sorolás elvégzése és dokumentálása az Informatikai Biztonsági Felügyelő feladata.

4.2.1. Osztályozási elvek kialakítása

Az adatokat értékük, a jogi előírások, a szervezet szempontjából képviselt érzékenységük és kritikusságuk szempontjából kell osztályozni.

Az adatokat az alábbi osztályokba kell sorolni:

- *Különlegesen érzékeny adatok* (titkok, „kiemelt” információvédelmi osztály): amelyekhez a belső és külső hozzáférést erősen korlátozni és szigorúan ellenőrizni, dokumentálni kell (pl. a rendszer biztonságát érintő adatok);
- *Érzékeny adatok* („fokozott” információvédelmi osztály): amelyekhez a belső és külső hozzáférést korlátozni, a hozzáférést naplózni kell (pl. elektronikus ügyintézés adatai, állampolgárok személyes adatai, stb.);
- *Belső adatok* („alap” információvédelmi osztály): amelyhez a külső hozzáférés nem lehetséges, a belső hozzáférés korlátozása nem kritikus;
- *Nyilvános, közhiteles adatok*: ahol a rendelkezésre állás és a megváltoztathatatlanság kritikus;
- *Nem osztályozott adatok.*

Az alkalmazásokat és az infrastruktúra elemeit a kezelt adatok biztonsági osztályával összhangban kell besorolni biztonsági osztályokba.

A fejlesztők és üzemeltetők a biztonsági besorolásnak megfelelő adminisztratív és technikai védelmet kell, hogy kialakítsanak.

4.2.2. Adatok jelölése és kezelése

Összhangban az elfogadott biztonsági osztályozási rendszerrel, megfelelő eljárásokat kell kidolgozni és bevezetni az adatok (információhordozók) jelölésére és kezelésére.

Az egyes biztonsági osztályokhoz az Üzemeltető egységes védelmi intézkedéseket határoz meg, amelyek végrehajtása is az Üzemeltető feladata.

Az olyan informatikai rendszerek vagy adatbázisok esetén, amelyek több adatcsoportot együtt tárolnak vagy dolgoznak fel, a rendszerben előforduló legmagasabb biztonsági osztály követelményeit kell érvényesíteni. Az informatikai rendszerek különböző környezetei (pl. éles, teszt, oktató rendszer) más-más biztonsági osztályba sorolhatók.

Azokat az adatokat, amelyeket az intézmény nem sorolt biztonsági osztályba, az Üzemeltető az „Alap" védelmi osztály követelményei szerint kezeli.

SZEMÉLYI BIZTONSÁG

5. fejezet

Cél: az informatikai biztonsági intézkedések végrehajtásával és ellenőrzésével kapcsolatos munkaköröket csak megfelelően ellenőrzött, megfelelően rögzített felelősség- és hatáskörrel felhatalmazott munkatársak töltsék be.

5.1. Ellenőrzött munkatársak alkalmazása

Az informatikai munkatársak munkába állása előtt a kezelt adatok érzékenységével arányos mélységű, a fontos és bizalmas munkakörökre vonatkozó szabályok szerinti ellenőrzést kell tartani.

A kockázattal arányos mértékben mérlegelni kell a munkatárs egyéni tulajdonságait is (pl. felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképesség, pánik-tűrőképesség, stb.).

A biztonsági szempontból kritikus informatikai munkaköröket betöltő munkatársak esetében az alkalmasságot rendszeresen felül kell vizsgálni.

Az érintett munkatársakkal olyan – az IBSZ szerinti tartalmú – *titokvédelmi nyilatkozatot* kell aláíratni, amely a munkaviszony megszűnte után is meghatározott időtartamig kötelezi őket a titoktartásra.

Külső szolgáltató igénybevétele esetén a *szerződésben vagy megállapodásban* kell rögzíteni a titoktartásra vonatkozó kötelezettségeket a kockázattal arányos módon.

5.2. Feladatok és felelősségi körök meghatározása

*Munkaköri leírások*ban, szabályzatokban kell rögzíteni az egyes munkakörökhöz tartozó feladatokat és felelősségi kört, a szükséges informatikai jogosultságokat. Minden munkakörhöz csak a munkához feltétlenül szükséges jogosultságokat kell megadni.

Biztonsági oktatást kell tartani a dolgozóknak alkalmazásukkor és új informatikai rendszerek bevezetésekor. Külön hangsúlyt kell fektetni a biztonságtudatosság fokozására.

A biztonsági szabályok megváltozásakor, de legalább kétévente frissítő oktatást kell tartani minden munkatárs számára.

5.3. Személyi biztonság az alkalmazás megszűnése, illetve megváltozása esetén

A munkatársak kilépése, tartós távolléte, a munkakör változása esetére eljárást kell kidolgozni a szükséges biztonsági intézkedésekről (jogosultság visszavonása, felfüggesztése, változtatása).

FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

6. fejezet

Cél: A védett erőforrásokhoz való illetéktelen hozzáférés elleni fizikai védelem kockázatarányos megvalósítása.

6.1. Területek védelme, biztosítása

6.1.1. Fizikai biztonsági zónák kialakítása

Biztonsági zónákat kell létrehozni annak megakadályozására, hogy jogosulatlan személyek hozzáférjenek az intézmény számára érzékeny adatokat, információkat, eszközöket tároló helyiségekhez, és ott károkat okozzanak.

A helyiségeket az alábbi biztonsági kategóriákba kell sorolni:

- Zárt terület (pl. gépterem),
- Kiemelt terület (pl. raktárak, áramellátó helyiségek),
- Ellenőrzött terület (pl. irodák, folyosók),
- Nyilvános terület (pl. ügyfélszolgálati tér).

A zónába sorolásnál tekintettel kell lenni arra, hogy a szomszédos helyiségek milyen biztonsági kategóriába tartoznak.

A biztonsági zónákhoz adminisztratív és védelmi intézkedéseket kell meghatározni.

6.1.2. Belépés- és mozgásellenőrzés

A különböző biztonsági zónák közötti mozgást ellenőrizni kell. A biztonsági zónához meghatározott követelményeknek megfelelő adminisztratív és műszaki eljárásokat kell alkalmazni.

A telephelyek kiválasztása és kialakítása során törekedni kell a közforgalmú (külső személyek által is használt) területek lehető legnagyobb mértékű elválasztására az üzemi területektől. Azokat a területeket, ahol külső személyek is tartózkodhatnak, nyilvános területként kell kezelni, és a hozzáférési pontokon és zónahatárokon az ennek megfelelő védelmet kell kialakítani.

Az ellenőrző pontok minimálisan a következő intézkedéseket kell megvalósítsák:

- személy azonosságának ellenőrzése,
- be- és/vagy kilépés időpontjának rögzítése.

Eljárást kell kidolgozni a belépés- és mozgásellenőrző rendszerek működtetésére és használatára.

6.2. Informatikai eszközök védelme

6.2.1. Berendezések elhelyezése és védelme

A berendezések elhelyezésére szolgáló helyiségek kiválasztásánál és kialakításánál figyelembe kell venni a berendezés biztonsági besorolása szerinti követelményeket. Meg kell határozni a környezeti hatások, szándékos támadás és véletlen károkozás kockázatát, és ennek megfelelő fizikai, elektronikai, és életerős védelmet kell biztosítani.

6.2.2. Közműszolgáltatások biztosítása

A közműszolgáltatások (pl. áram) kiesése esetére a szolgáltatási szint megállapodásokkal és a katasztrófa-elhárítási eljárásokkal összhangban kell kiválasztani a szükséges műszaki megoldásokat (pl. áramellátás: szünetmentes áramforrás, többirányú betáplálás, áramtermelő generátor).

6.2.3. A kábelezés biztonsága

A kábelek elhelyezésekor, a használt anyagok kiválasztásakor figyelembe kell venni a kiszolgált informatikai erőforrások biztonsági besorolását.

A kábeleket a várható fizikai igénybevételnek és a továbbított adatok kritikusságának megfelelően kell védeni, figyelembe véve az elektromágneses sugárzások beilletve kijutása (zavar, illetve információ) elleni védelmet is.

A kritikus erőforrások között redundáns kapcsolatot kell kialakítani (különböző fizikai útvonalak kijelölésével).

6.2.4. Berendezések karbantartása

A berendezések karbantartására karbantartási tervet kell készíteni, amely biztosítja a berendezések előírt (idő vagy igénybevételi) intervallumként történő szakszerű karbantartását.

6.2.5. Berendezések biztonságos selejtezése és újrafelhasználása

Olyan selejtezési és megsemmisítési eljárásokat kell kidolgozni, amelyek biztosítják, hogy a selejtezett eszközökön tárolt információk visszaállítása ne legyen lehetséges.

A KOMMUNIKÁCIÓ ÉS AZ ÜZEMELTETÉS IRÁNYÍTÁSA

7. fejezet

Az üzemeltetési tevékenységek végrehajtásának és ellenőrizhetőségének biztosítása

7.1. Üzemeltetési eljárások és felelősségi körök

7.1.1. Dokumentált üzemeltetési eljárások

Az üzemeltetési feladatok határidőre történő, szabályozott végrehajtása érdekében üzemeltetési szabályzatot és üzemeltetési eljárásokat kell készíteni.

Az üzemeltetési szabályzatban az üzemeltetéssel kapcsolatos feladatokat és felelősségeket kell meghatározni.

Az üzemeltetési eljárásokban az üzemeltetéssel kapcsolatos feladatok végrehajtási eljárásait, műszaki leírásait kell meghatározni.

7.1.2. Változáskezelési eljárások

Ki kell dolgozni a változások kezelésének szabványos folyamatát az igényfelvételtől az átadás-átvételig.

A változáskezelési eljárás tartalmazza legalább az alábbiakat:

- változási igények fogadása, kezelése,
- kockázat elemzése,
- változás dokumentálása és implementálása.

7.1.3. Feladatkörök, kötelezettségek elhatárolása

Meg kell határozni a biztonsági szempontból összeférhetetlen feladatokat, amelyek véletlen vagy szándékos károkozást tesznek lehetővé, és ezek szétválasztását érvényesíteni kell a szervezeti felépítésben, valamint a munkakörök kialakításakor.

Összeférhetetlen feladatkörök (például):

- fejlesztés és üzemeltetés,
- üzemeltetési és biztonsági adminisztráció,
- üzemeltetés és felhasználás.

7.1.4. Fejlesztési, teszt és üzemeltetési berendezések különválasztása

A fejlesztési, teszt környezeteket és az üzemi környezetet logikailag és lehetőség szerint fizikailag is szét kell választani egymástól.

7.2. Harmadik felek tevékenységének irányítása

7.2.1. Szolgáltatásnyújtás

Meg kell határozni azokat a szerződéses elemeket és tevékenységeket, amelyeket érvényesíteni kell a harmadik felekkel kötött szolgáltatási szerződésekben. Ki kell dolgozni ezen követelmények teljesülésének ellenőrzési eljárásait.

7.2.2. Harmadik felek szolgáltatásainak figyelemmel kísérése és átvizsgálása

Ki kell dolgozni a szolgáltatási szintek leírásának, érvényesítésének, a teljesítés dokumentálásának, ellenőrzésének és a nem megfelelő teljesítés szankcionálásának eljárásait.

7.2.3. Harmadik felek szolgáltatásaival kapcsolatos változások kezelése

Ki kell dolgozni a változáskezelési eljárásokat a külső fél által nyújtott szolgáltatásokra. A változáskezelési eljárásnak biztosítania kell a következőket:

- a változások végrehajtása csak a megfelelő jóváhagyás után történjen,
- a végrehajtás során is érvényesüljenek a biztonsági követelmények,
- az átvétel során ellenőrzésre kerüljön a specifikációban/változási kérelemben leírtak teljesülése.

7.3. Rendszertervezés és -elfogadás

7.3.1. Kapacitás-menedzsment

Ki kell dolgozni az erőforrás-kihasználtság figyelésének, ellenőrzésének, elemzésének és a jövőbeli trendek előrejelzésének folyamatait, és ennek eredményét figyelembe kell venni az erőforrás-beszerzések tervezésekor.

7.3.2. Rendszerek elfogadása, átvétele

A rendszerek átvételéhez olyan eljárásokat kell kidolgozni, amelyek biztosítják az elvárásoknak való megfelelés ellenőrzését. Az ellenőrzés módszerei a (funkcionális, terheléses, stb.) tesztelés, forráskód-audit, szakértői ellenőrzés stb.

7.4. Védelem a rosszindulatú és mobil kódok ellen

7.4.1. Rosszindulatú kód elleni védelem

Olyan adminisztratív és technikai intézkedéseket kell alkalmazni, amelyek megakadályozzák a rosszindulatú kódokat tartalmazó programok bejutását, alkalmazását.

7.4.2. Mobil kód elleni intézkedések

Le kell tiltani minden olyan kód futtatását, amelyek nem szükségesek a felhasználók munkájához.

7.5. Biztonsági mentés

7.5.1. Információk biztonsági mentése

Olyan mentési rendet kell kialakítani, amely biztosítja az adatok visszaállíthatóságát a szervezet által meghatározott követelmények szerint (elvárt visszaállítási idő, maximálisan elviselhető adatvesztés, stb.).

A mentések gyakoriságát, a mentés módját, a használt adathordozót és a tárolási helyet a fentiek figyelembevételével kell kiválasztani, és ki kell dolgozni azokat az eljárásokat, amelyek teljesítik a követelményeket.

Az eljárások kidolgozása után az érintettek számára oktatás szükséges, és elengedhetetlen a teljes visszaállítási eljárás tesztelése is.

Ki kell dolgozni a mentések ellenőrzésének rendjét is.

7.6. Hálózatbiztonság kezelése

7.6.1. Hálózatok védelme

A hálózatok biztonsága érdekében a következő intézkedések megvalósítása javasolt: a hálózat szegmentációja, tűzfalas védelem, vírusvédelmi eszközök, tartalomszűrés, titkosított adatvédelmi csatornák kialakítása.

A hálózati rendelkezésre állás érdekében a hálózati forgalmat rendszeresen mérni és értékelni kell, és biztosítani, hogy a szükséges sávszélesség kellő biztonsággal rendelkezésre álljon.

Dokumentálni kell a hálózatokon alkalmazott védelmi intézkedéseket és azok üzemeltetési eljárásait.

7.6.2. Hálózati szolgáltatások biztonsága

Dokumentálni kell a hálózati szolgáltatásokkal szemben támasztott biztonsági követelményeket és azok ellenőrzésének, valamint a nem megfelelő teljesítés szankcionálásának eljárásait is.

7.7. Adathordozók kezelése

7.7.1. Adathordozók kezelése

Ki kell dolgozni valamennyi adathordozó kezelésének eljárásait, kiemelt figyelmet fordítva a telephelyen kívüli védelemre. A szabályzatnak ki kell terjedni a teljes élettartamra, a nyilvántartásra, a selejtezésre, a frissítésre, több példány készítésére. Kiemelt figyelmet kell fordítani az USB eszközökre, a memóriakártyákra.

7.7.2. Adathordozók selejtezése

Olyan selejtezési eljárásokat kell kidolgozni, amelyek biztosítják a selejtezett adathordozókon tárolt adatok biztonságos, visszaállítást lehetetlenné tevő megsemmisítését. Minden adathordozó-típusra ki kell dolgozni a specifikus eljárásrendet.

A selejtezés folyamatát dokumentálni kell a későbbi ellenőrizhetőség érdekében.

7.7.3. Informatikai rendszerekben tárolt adatok kezelési eljárásai

Minden biztonsági osztályra ki kell dolgozni az adatok tárolási és kezelési eljárásait, amelyek biztosítják a biztonsági osztály előírásai szerinti védelmet.

7.7.4. Rendszerdokumentáció védelme

Ki kell dolgozni a rendszerek dokumentációjának tárolási és hozzáférési szabályait, ami biztosítja azok rendelkezésre állását és a jogosultsághoz kötött, ellenőrzött hozzáférést. A rendelkezésre állásba bele kell érteni a naprakészséget, a változások átvezetésének folyamatszerű és biztonságos mechanizmusát is. A tárolási rendnek azt is biztosítania kell, hogy szükség esetén az arra jogosultak azonnal hozzáférhessenek a szükséges dokumentációhoz.

7.8. Adatcsere, adattovábbítás

7.8.1. Adatcserére, adattovábbításra vonatkozó szabályzatok és eljárások

Ki kell dolgozni a külső szervezetekkel történő adatcsere, a részükre történő adattovábbítás technikai és adminisztratív eljárásait. Az alkalmazott védelmet az átadott információ biztonsági besorolásának megfelelően kell kialakítani. Az eljárásnak ki kell térnie az adatkéréstől az adat megérkezésének visszaigazolásáig minden lépésre, és egyértelműen definiálnia kell a folyamatban résztvevők felelősségét.

7.8.2. Megállapodások az adatcseréről, adattovábbításról

Az adatcsere, adattovábbítás biztonságáról a szervezetek között olyan megállapodást kell kötni, amely mindkét fél által támasztott követelményeknek megfelel.

7.8.3. Fizikai adathordozók szállítása

Ki kell dolgozni az adathordozók szállítására vonatkozó szabályzatot. A szállításhoz használt eszközt, járművet és adminisztratív védelmet a szállított adat érzékenysége és kritikus volta alapján kell meghatározni.

7.8.4. Elektronikus üzenetek küldése/fogadása

Biztosítani kell az elektronikus üzenetekben továbbított információk biztonságát és rendelkezésre állását. Ehhez meg kell határozni azokat az eljárásokat, amelyeket az elektronikus üzenetek továbbítása során alkalmaznak.

7.8.5. Működést támogató információs rendszerek

Szabályozni kell a rendszerek használatát azok túlterhelésének, üzemzavarainak elkerülése, illetve a tárolt információk sérülésének megakadályozása érdekében. Meg kell határozni, hogy az érintett rendszerek ki által, milyen célra és módon alkalmazhatók (pl. internethasználat, e-mail használat).

7.9. Valós idejű, ügyfeleknek nyújtott szolgáltatások

7.9.1. On-line üzenetváltások (tranzakciók)

Ki kell dolgozni az on-line tranzakciók védelmére vonatkozó követelményeket, és a követelmények teljesítése érdekében végrehajtott technikai és adminisztratív intézkedéseket.

7.9.2. Nyilvánosan hozzáférhető információk

Ki kell dolgozni a nyilvánosan hozzáférhető információk (pl. honlapok, nyilvános adatbázisok) sértetlensége érdekében szükséges adminisztratív és technikai intézkedéseket. Ki kell térni az információ változtatásának eljárásrendjére, új információ közzététele előtt követendő eljárásra és egyes információk törlésének eljárásaira is.

7.10. Követés (monitoring)

7.10.1. Audit naplózás

Meg kell határozni, hogy milyen adatok hozzáférése/módosítása esetén van szükség és milyen mélységű naplózásra. Ki kell dolgozni a naplófájlok kezelésére (rögzítés, elemzés) vonatkozó adminisztratív eljárásokat és technikai eljárásokat.

A kritikus rendszerek naplófájljait rendszeresen vizsgálni kell az esetleges üzemzavarok és támadási kísérletek felfedése érdekében. Ez a vizsgálat részben automatizálható, amennyiben a naplófájlok mennyisége ezt indokolja.

7.10.2. Rendszerhasználat figyelése

Ki kell dolgozni a rendszerhasználat figyelésének (adatgyűjtés-elemzés-intézkedés) eljárásait, amelyek biztosítják, hogy a rendellenességek időben feltárásra kerüljenek és kezelhetők legyenek.

7.10.3. Naplóinformációk védelme

Ki kell dolgozni a rendszernaplók rögzítésének, tárolásának és elemzésének eljárásait, amelyek biztosítják azok sértetlenségét, megváltoztathatatlanságát és a jogosultságához kötött hozzáférést.

7.10.4. Adminisztrátori és kezelői naplók

Ki kell dolgozni az adminisztrátori és operátori naplók rögzítésének és tárolásának eljárásait, amelyek biztosítják azok sértetlenségét, megváltoztathatatlanságát és a jogosultsághoz kötött hozzáférést.

7.10.5. Hibák naplózása

Ki kell dolgozni a hibákra vonatkozó információk rögzítésének, tárolásának és elemzésének eljárásait.

A hibaelemzések alapján meg kell hozni a szükséges javító intézkedéseket (hiba megkeresése az adott rendszerben, kapacitásbővítés, stb.).

7.10.6. Időadatok szinkronizálása

Biztosítani kell, hogy a különböző rendszerekben rögzített adatok (tranzakciók, naplóbejegyzések, üzenetek) időadatai a lehető legteljesebb összhangban legyenek.

HOZZÁFÉRÉS-ELLENŐRZÉS

8. fejezet

Cél: a dokumentumokhoz, információkhoz, adatokhoz, szolgáltatásokhoz és rendszerekhez történő hozzáférés felügyelete, ellenőrzése.

8.1. Hozzáférési szabályok kialakítása

8.1.1. Hozzáférés-ellenőrzési szabályzat

Hozzáférés-ellenőrzési szabályzatot kell kialakítani, bevezetni és betartatni. A szabályzat periodikus felülvizsgálata és módosítása elengedhetetlen. Minden felhasználó csak azokhoz az erőforrásokhoz, információkhoz férhessen hozzá, amelyek munkájához mindenképpen szükségesek.

8.2. Felhasználói hozzáférés irányítása

8.2.1. Felhasználók regisztrálása

Ki kell dolgozni, be kell vezetni és szigorúan be kell tartatni a felhasználói jogosultságok kiadásának és visszavételének a rendszerét - lehetőleg az egyes felhasználók igénybevételi, csatlakozási szerződéséhez kötve. A felhasználók hozzáférési jogait rendszeresen át kell tekinteni, hogy minden felhasználó csakis azokhoz az információkhoz férhessen hozzá, amely munkájához aktuálisan szükséges.

8.2.2. Speciális jogosultságok kezelése

Az általános összeférhetetlenségi szabályoktól való erős eltérést korlátozni kell, az ilyen jogosultságok kiadását mindenképpen kerülni kell. Amennyiben valamely elkerülhetetlen ok miatt mégis létre kell hozni ilyet, akkor azt csak dokumentáltan, és csak a feltétlenül szükséges időtartamra szabad megadni.

8.2.3. Felhasználói jelszavak kezelése, gondozása

A jelszavak felhasználói kezelését szabályozni kell, figyelve arra, hogy a felhasználók titokban tartsák és megfelelő időközönként változtassák jelszavaikat, valamint biztosítani kell, hogy a jelszavak kiosztásakor, illetve használatakor csakis a tulajdonos szerezzen tudomást a jelszóról.

8.3. Felhasználói felelősségek

8.3.1. Jelszóhasználat

A felhasználók számára olyan használati rendet kell kialakítani, amely biztosítja a megfelelő erősségű jelszavak használatát és ezen jelszavak megfelelő gyakoriságú cseréjét.

8.3.2. Őrizetlenül hagyott felhasználói berendezések kezelése

A külső felhasználókat a kapcsolati alrendszerek megfelelő kialakításával, a belső felhasználókat (alkalmazottakat) szabályzatokkal kell kötelezni arra, hogy ha őrizetlenül hagyják a berendezéseiket, akkor (akár logikailag, akár fizikailag) zárják le azokat.

A belső felhasználókat kötelezni kell arra, hogy csak az aktuális munkához szükséges dokumentumokat tartsák az asztalon/képernyőn, és ne hagyják ezeket a dokumentumokat, adatokat felügyelet nélküli hozzáférhető helyen.

8.4. Hálózati hozzáférések kezelése, ellenőrzése

8.4.1. Hálózati szolgáltatások használatára vonatkozó szabályzat

A hálózati szolgáltatások használatáról szabályzatot kell készíteni, s azt be kell tartatni. A szabályzat tartalmazza, hogy milyen felhasználói kör milyen hálózati területhez férhet hozzá.

8.4.2. Felhasználó hitelesítése külső hozzáférés esetén

A külső összeköttetéseket csak a feltétlenül munkaidőn is elérni szükséges rendszerekhez szabad engedélyezni, s kriptográfiai védelmi módszereket kell alkalmazni.

8.4.3. Távdiagnosztikai és konfigurációs portok védelme

A távdiagnosztikai és konfigurációs portokhoz való fizikai és logikai hozzáférést ellenőrizni, szabályozni kell. A hozzáféréshez a rendszerben alkalmazott legszigorúbb azonosítási eljárásokat és naplózási rendet kell használni.

8.5. Operációs rendszerekhez való hozzáférés szabályozása

8.5.1. Biztonságos bejelentkezési eljárások

Az operációs rendszerekbe való bejelentkezési eljárásokat – a jogosulatlan hozzáférés, a szándékos károkozás elkerülése érdekében – szabályozni kell. Fontos a különböző szerepköröknek megfelelő hozzáférési jogosultság meghatározása és az ezekhez tartozó jogok beállításának szabályozása (igénylés, engedélyezés, beállítás, visszavonás).

8.5.2. Felhasználók azonosítása és hitelesítése

A felhasználók egyedi azonosítására, hitelesítésére megbízható rendszert kell választani, annak használatát szabályzatban kell rögzíteni, betartását szigorúan meg kell követelni. A szabályzatnak ki kell terjednie az azonosítás és hitelesítés teljes életciklusára.

Meg kell határozni a biztonságos jelszóra vonatkozó követelményeket, szabályozni kell a jelszavak létrehozására, módosítására, tárolására, használatára, visszavonására vonatkozó eljárásokat. A felhasználók jelszóhasználattal kapcsolatos feladata-

it és kötelezettségeit szintén szabályzatba kell foglalni, és rendszeresen ellenőrizni kell annak betartását.

8.5.3. Rendszer-segédprogramok használata

A rendszer-segédprogramok használata különösen veszélyes lehetőségeket teremt nehezen ellenőrizhető manipulációkra, ezért ezek használatát különös figyelemmel kell szabályozni, és a szabályzatban foglaltakat ellenőrizni. A fejlesztő eszközökhöz, az adatbázisokhoz közvetlen hozzáféréseket lehetővé tevő segédprogramokhoz való hozzáférés csak nagyon indokolt esetben engedélyezhető, a tevékenység végén az engedélyt vissza kell vonni, és lehetőleg ki kell zárni az ellenőrizhetetlen származású programok használatát.

8.5.4. Az összeköttetés/kapcsolat idejének korlátozása

Szabályozni kell, hogy mekkora az inaktív vagy teljes időtartam, amely után az adatkapcsolatot meg kell szüntetni. Ezt az időintervallumot figyelembe kell venni a rendszerek paraméterezésénél, illetve az alkalmazások fejlesztésénél. Az időtartam betartandó attól függetlenül, hogy humán beavatkozásról vagy alkalmazás automatikus aktivitásáról van szó.

8.6. Alkalmazói rendszerekhez való hozzáférés felügyelete

8.6.1. Az adat-hozzáférés korlátozása

Alkalmazás-funkciónként, illetve egyes (pl. adatminősítés, biztonsági szint szerinti) adatkörökre vonatkozó hozzáférés szabályozása, a jogosulatlanok kizárása. Fontos az egyes manipulációk, jogosulatlan kísérletek naplózása és a naplóállomány rendszeres értékelése. A korlátozások lehetőségét az alkalmazás fejlesztésének időszakában kell megtervezni és az alkalmazást ennek megfelelően implementálni.

8.6.2. Érzékeny adatokat kezelő rendszerek elkülönítése

Az egyes rendszereket kategóriákba kell sorolni az általuk kezelt adatok érzékenységének megfelelően. Az érzékenynek minősített adatokat kezelő alkalmazás elkülönítésével hozható létre a szükséges biztonsági szint. A rendszerek besorolását rendszeresen felül kell vizsgálni és aktualizálni kell.

8.7. Mobil eszközök használata és távmunka

8.7.1. Mobil számítógép használata és a vele történő kommunikáció

A mobil számítógépek biztonságos használatának szabályozása. A hozzáférés, a logikai és fizikai biztonság, az adatmentések megvalósítása, illetve a biztonságos környezeten kívüli munkavégzés szabályrendszere is meghatározandó.

8.7.2. Távmunka

Szabályozni kell, hogy a biztonságos távoli hozzáférés, illetve munkavégzés érdekében milyen tevékenységek és technikai feltételek szükségesek. Távoli hozzáférés és munkavégzés csak indokolt esetben engedélyezhető, és a hozzáférés, adatcsere biztonsága érdekében külön eljárásokat kell meghatározni és megvalósítani.

AZ INFORMATIKAI RENDSZEREK FEJLESZTÉSE ÉS KARBANTARTÁSA

9. fejezet

9.1. Informatikai rendszerek informatikai biztonsági követelményei

9.1.1. Biztonsági követelmények elemzése és meghatározása

A fejlesztés vagy beszerzés kezdete előtt, az informatikai rendszerekre vonatkozó biztonsági kockázatokat elemezni kell, ez alapján meg kell határozni a vonatkozó biztonsági intézkedéseket.

9.2. Biztonságos adatfeldolgozás az alkalmazási rendszerekben

9.2.1. Bemenő adatok érvényesítése

Az informatikai rendszerek bemenő adatainak ellenőrzése mind tartalmi, mind formai szempontból.

9.2.2. Az adatfeldolgozás ellenőrzése

Az alkalmazásokba érvényességi ellenőrzéseket kell beépíteni, hogy észlelni lehessen az információkat érő, feldolgozási hibából vagy akár szándékos cselekedetekből adódó bármilyen sérülését.

9.2.3. Üzenetek hitelessége és sértetlensége

Meg kell határozni, hogy az alkalmazások közti kommunikáció során milyen eszközökkel lehet biztosítani a sértetlenséget és hitelességet (pl. aszimmetrikus kulcsú digitális aláírás, titkosítás, időbélyegek alkalmazása), illetve hogy ezen óvintézkedések mely üzenettípusok esetében szükségesek. A meghatározott eszközök alkalmazását szabályozni kell.

9.2.4. Kimenő adatok hitelesítése

Szükséges annak biztosítása, hogy mind az automatikus, mind a manuális illesztő felületeken a megfelelő időben, a megfelelő (szabályozott) struktúrában és adattartalommal jelenjen meg a kimenő információ.

9.3. Titkosítási intézkedések

9.3.1. Titkosítási eljárások használatára vonatkozó szabályzat

Ki kell alakítani és alkalmazni kell a titkosítási eljárások használatára vonatkozó szabályzatot. A szabályzat betartását ellenőrizni kell. A védelem szükséges szintjét a kockázat-analízisre kell alapozni.

9.3.2. Kulcsmenedzsment

A magyar jogi szabályozásnak megfelelő, lehetőleg az EU gyakorlatának és ajánlásainak is eleget tevő kriptográfiai technikákon alapuló kulcsmenedzsment-rendszert kell kialakítani.

9.4. Rendszerállományok biztonsága

9.4.1. Üzemelő szoftverek ellenőrzése

Szabályzatba kell foglalni a szoftverek telepítésének és üzemeltetésének elvárt folyamatát. Létre kell hozni a központi szoftverkatalógust, s csak az abban szereplő (előzetesen bevizsgált) szoftvereket szabad a számítógépekre telepíteni. Biztosítani kell, hogy a fejlesztők és karbantartók csak azokhoz a rendszerekhez férjenek hozzá, amelyekre munkájukhoz feltétlenül szükség van.

9.4.2. A rendszervizsgálat adatainak védelme

A rendszer vizsgálatához szükséges adatok körét gondosan kell megválasztani, azokat teljes életútjuk során folyamatosan védeni és ellenőrizni kell. A személyes adatokat tartalmazó üzemeltetési, tesztelési adatbázisok használatát el kell kerülni.

9.4.3. Programok forráskódjához való hozzáférés ellenőrzése

A használt programok forráskódját biztonságos helyen kell tárolni, a hozzáférést szigorúan korlátozni és naplózni szükséges. Amennyiben a forráskód nem ellenőrizhető, az önmagában is kockázati tényezőt jelent.

9.5. Informatikai biztonság a fejlesztési és karbantartási folyamatokban

9.5.1. Változás-kezelés

A változások végrehajtására változás-kezelési eljárásokat kell bevezetni és betartani. Minden változtatást ellenőrizni és dokumentálni kell.

9.5.2. Az üzemelő rendszerek megváltoztatását követő ellenőrzések

A használatban levő rendszerek megváltozásakor, az operációs rendszer alapértelmezett átvizsgálása után – meg kell vizsgálni, hogy (főleg a működés szempontjából kritikus) alkalmazások működésére az adott változás nincs-e káros hatással.

9.5.3. Szoftvercsomagok megváltoztatásának korlátozása

Minél alacsonyabb szinten kell tartani a szoftvercsomagok változtatását. Valamennyi változtatás szükségességét, indokoltságát ellenőrizni kell. Változtatás esetén az eredeti verziót meg kell őrizni, s a fejlesztést egy másolaton kell elvégezni. Az új verziót alapos tesztelés alá kell vetni, éles bevezetése csak ez után történhet.

9.5.4. A rendszerinformációk kiszivárgásának megelőzése

Az információk kiszivárgásának megelőzése érdekében minden rendelkezésre álló forráskódot be kell vizsgálni/vizsgáltatni használat előtt. Csak tiszta forrásból szabad programokat beszerezni. Csak ezen vizsgálatok eredményének ismeretében szabad bármely programot a végleges rendszerbe engedni.

9.5.5. Kihelyezett szoftverfejlesztés

Kiemelt figyelemmel kell kísérni a külső szoftverfejlesztést, a kapott programot alaposan felül kell vizsgálni/vizsgáltatni. Csak megbízható forrásból származó szoftvert szabad alkalmazni, különös figyelemmel a szoftver- és szellemi tulajdonjogokra.

9.6. Műszaki sebezhetőségek kezelése

9.6.1. A műszaki sebezhetőségek ellenőrzése

Fel kell mérni az alkalmazott rendszerek sebezhető pontjait, s az ebből fakadó kockázatokat – megfelelő védelmi intézkedések meghozatalával – meg kell szüntetni (illetve a kockázattal arányosan minimalizálni).

INFORMATIKAI BIZTONSÁGI ESEMÉNYEK (INCIDENSEK) KEZELÉSE

10. fejezet

10.1. Informatikai biztonsági események és sérülékenységek jelentése

Rendelkezni kell a biztonsági események osztályozására és jelentésére vonatkozó eljárással. A biztonsági események értékelése és osztályozása az alapja a megfelelő védelmi eljárások kialakításának.

Ki kell dolgozni a biztonsági események kezelési eljárását, amely legalább a következőket tartalmazza:

- a biztonsági sérülékenységek jelentésére vonatkozó eljárást,
- a biztonsági események értékelésére vonatkozó eljárást,
- a biztonsági eseményről szóló információ megfelelő szintre történő eljuttatásának biztosítását,
- a fenti feladatok ellátásáért felelős személy adatait.

Az eseménykezelést be kell illeszteni a működési környezetbe (Helpdesk).

10.2. Informatikai biztonsági események jelentése

A feltárt és dokumentált eseményeket gyűjteni és rendszeresen értékelni kell. Az események okozta hibákat analizálva meg kell határozni a hibák okát. Ki kell dolgozni egy hatékony és gyors eljárást a problémák megismerésére, hogy minél előbb kezelhetővé váljanak.

Eljárásokat kell kidolgozni, és felelősöket kell megnevezni az informatikai biztonsági események kezelésére.

Az események kezelése be kell épüljön az üzemeltetés rendjébe. A feltárt események értékelését (osztályozását) biztosító rendszert kell kialakítani.

Az események kezeléséhez bizonyítékokat kell gyűjteni, a megtett intézkedéseket dokumentálni kell annak érdekében, hogy a később előforduló hasonló eseményeket már a kialakított módon lehessen kezelni vagy megelőzni.

10.3. Informatikai Biztonsági problémakezelési eljárás kialakítása

Eljárásokat kell kidolgozni, és felelősöket kell megnevezni az informatikai biztonsági problémák megállapítására és kezelésére.

A fellépő események okozta hibák értékelése mutathat rá a hiba okára, vagyis a problémára.

A problémák ellen védelmi intézkedéseket kell hozni, az általuk képviselt kockázatok arányában.

A teljes eljárást menedzselni kell, vagyis ki kell alakítani a folyamatot, és felelőst kell rendelni hozzá. Gondoskodni kell az esemény, hiba, probléma nyilvántartásáról annak érdekében, hogy a későbbiekben a hasonló események, illetve hibák esetén már a tapasztalatból kiindulva lehessen intézkedni.

A MŰKÖDÉS FOLYTONOSSÁGÁNAK IRÁNYÍTÁSA

11. fejezet

11.1. A működés-folytonosság biztosítása

Működés-folytonossági eljárásokat kell kidolgozni és dokumentálni.

A dokumentumban azonosítani kell

- a kritikus informatikai szolgáltatásokat,
- az informatikai szolgáltatások megengedett kiesési idejét,
- a minimális szolgáltatási szintet,
- átmeneti eljárásokat,
- az informatikai szolgáltatás visszaállítására vonatkozó eljárásokat.

Meg kell határozni azokat az infrastruktúrákat és szolgáltatásokat, amelyeknek működniük kell lokális események/katasztrófák esetén is, hogy ezáltal nyújtsanak informatikai támogatást az esemény elhárításához. Ezekre nézve ki kell alakítani a megfelelő tartalékokat. Szabályozni kell működtetésüket és használatukat, és rendszeresen vizsgálni kell a működésképességüket. Az eljárást tesztelni kell és a dokumentumot évente, illetve a releváns változások alkalmával felül kell vizsgálni.

11.2. Informatikai katasztrófa-elhárítási terv

A katasztrófa-elhárítási terv kiterjed:

- a kritikus informatikai erőforrások azonosítására,
- az elviselhető kiesési időablak meghatározására,
- az erőforrások pótlására/visszaállítására történő eljárások kialakítására az időablakon belül,
- a felkészülés, a válasz és a visszaállítás feladatainak meghatározására, a felelősök hozzárendelésére.

Az eljárásokat tesztelni kell, és a dokumentumot évente, illetve a releváns változások alkalmával felül kell vizsgálni.

MEGFELELÉS A JOGSZABÁLYOKNAK ÉS SZABÁLYOZÓKNAK

12. fejezet

12.1. Jogszabályi követelményeknek való megfelelés

Az informatikai működés során fenn kell tartani a jogszabályi megfelelést. Szükséges az informatikai működésre hatással levő jogszabályok azonosítása, és a megfelelés dokumentálása. Eljárást kell kidolgozni a megfelelés fenntartására, az időszakos (évenkénti) felülvizsgálatra.

12.2. Az informatikai biztonsági szabályzatnak, szabványoknak és műszaki követelményeknek való megfelelés

Eljárást kell kidolgozni a biztonsági szabályzatnak, szabványoknak való megfelelés ellenőrzésére.

12.3. Az informatikai rendszer biztonsági auditálásának (felülvizsgálatának) szempontjai

Ki kell dolgozni a védelmi intézkedések felülvizsgálatának rendszerét, kitérve az alkalmazott felülvizsgálati eljárásra, gyakoriságára, valamint az érintettek felelősségére és feladataira.

Javasolt külső, független szakértőt bevonni az ellenőrzésbe.

ZÁRÓ RENDELKEZÉSEK

13. fejezet

1. Jelen dokumentumot a Szenátus 81/2009. (XI.4.) számú határozatával jóváhagyta.

2. A dokumentum rendelkezéseit 2009. november 4-től kell alkalmazni., melyek módosításig, illetve visszavonásig hatályosak.

Eger, 2009. november 4.

Dr. Hauser Zoltán
rektor

MELLÉKLETEK

1. sz. melléklet

Informatikai biztonsági alapelvek

Az **informatikai biztonság** az informatikai rendszer olyan – az érintett[3] számára kielégítő mértékű – állapota, amelynek védelme az infokommunikációs rendszerben kezelt[4] adatok *bizalmassága, sértetlensége* és *rendelkezésre állása*, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folyamatos, és a kockázatokkal arányos, valamint a hatályos jogszabályoknak megfelelő. (Röviden: az informatikai rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának[5] védelme).

Az adatok **bizalmassága** azt jelenti, hogy azokhoz csak az arra jogosultak, kizárólag az előírt módokon férhetnek hozzá, illetve rendelkezhetnek azok felhasználásáról. (Nem fordulhat elő úgynevezett jogosulatlan információszerzés).

A **hitelesség** azt jelenti, hogy a szervezet belső, vagy más szervezetekkel fenntartott kapcsolataiban a partnerek kölcsönösen és kétségtelenül felismerik egymást és ezt az állapotot a kapcsolat egész idejére változatlanul fenntartják.

Az információk vagy a programok **sértetlensége** alatt azt értjük, hogy az információkat/programokat csak az arra jogosultak változtathatják meg, és azok véletlenül sem módosulhatnak. (A sértetlenségen fogalma alatt gyakran értik a sértetlenségen túli *teljességet*, továbbá az *ellentmondás-mentességet* és a korrektséget, együttesen: az **integritást**. Az integritás itt azt jelenti, hogy az információ valamennyi része elérhető).

Rendelkezésre állás az informatikai rendszer(elem) – ide értve az adatot is – azon tulajdonsága, amely szerint az informatikai rendszer(elem) a szükséges időben és időtartamra használható (vagyis amikor az adatokhoz való jogosult hozzáférés, illetve a rendszer működőképessége nincs akadályozva).

Teljes körű a védelem: ha a védelmi intézkedések az informatikai rendszer összes elemére kiterjednek.

Zárt a védelem: ha az összes, releváns fenyegetést figyelembe vevő védelmi rendszer kerül kialakításra.

Folyamatos a védelem: ha a védelem az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

Kockázattal arányos a védelem: ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

Informatikai kontroll: mindazon szabályok, eljárások, gyakorlati módszerek, és szervezeti struktúrák, amelyeket arra a célra terveztek, hogy kellő megerősítést nyújtsanak arra vonatkozóan, hogy az „üzleti" célkitűzéseket megvalósítsák, és a nem kívánatos eseményeket megelőzzék, vagy felderítsék és korrigálják.

---

[3] Az érintett alatt a védelem nem kielégítő megvalósítását elszenvedő, a védelmet előíró, továbbá a védelemért felelős személyek és szervezetek együttese értendő.

[4] Az adatok kezelése az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele, tárolása, feldolgozása (megváltoztatás, átalakítás, összegzés, elemzés, stb.), továbbítása, törlése, hasznosítása (ide értve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozása.

[5] Ezt a hármas elvárást szokás az angol rövidítések alapján CIA-elvnek nevezni: Confidentiality, Integrity, Availability.

AZ INFORMATIKAI BIZTONSÁGI HELYZETFELMÉRÉS ÉS AKCIÓTERVEZÉS ELVÉGZÉSÉNEK MÓDSZERTANI ELEMEI

1. Az IT biztonsági helyzetfelmérés célja

Az IT biztonsági helyzetfelmérés célja az információk bizalmasságának, integritásának, rendelkezésre állásának mértékét befolyásoló sebezhetőségek és kockázatok feltárása. (A felmérés során kitérünk az informatikai rendszerekben és a papíron tárolt információk biztonsági szempontjaira is).

A kérdéslista alapvetően alkalmazkodik a COBIT információbiztonsági módszertanához.

Az informatikai biztonsággal kapcsolatban vizsgálandó szempontokat a következő 4 csoportba soroltuk:

- Szervezeti és humán veszélyforrások és intézkedések;
- Adminisztratív biztonsági veszélyforrások és intézkedések;
- Fizikai biztonsági veszélyforrások és intézkedések;
- Logikai/technikai biztonsági veszélyforrások és intézkedések.

2. A biztonsági helyzetfelmérés módszere

2.1. A biztonsági helyzetfelmérés hatóköre

A szervezet kulcsszereplőinek illetve kritikus erőforrásainak felmérését az alábbi módszerekkel és eljárások segítségével végezzük el:[6]

- Interjúk lefolytatása
- Helyszíni szemlék és bejárások.

Ennek során megismerhető az információbiztonság jelenlegi helyzete. Fókusz-területek:

- Informatika
- Humán szakterület
- Adminisztratív szakterület
- Fizikai környezet.

2.2. Veszélyforrások, fenyegetettségek meghatározása

A helyzetfelmérés megállapításai alapján meghatározhatók azok a veszélyforrások, amelyek veszélyeztetik a szervezet informatikai működését és információvagyonát.

2.3. Sebezhetőségek meghatározása

Azok a gyenge pontok, amelyeken keresztül a rendszer támadható, ahol a fenyegetettségek realizálódhatnak és kár keletkezhet. (Pl. nem naprakész frissítések, patch-ek; nem teljes körű, nem egyenszilárdságú védelem; tűzfal hiányosságai; védelmi megoldások, kontrollok, szoftver, hardver elem, komponens hiánya.)

---

[6] Az EKF informatikai működését és biztonságra vonatkozó szabályait az OKM által 2008-ban végzett informatikai rendszerellenőrzésről készített 4764-2/2008. sz. jelentés értékelte.

2.4. Megoldási javaslatok megfogalmazása

A helyzetfelmérés és a veszélyforrások elemzésének eredményeire támaszkodva – figyelembe véve bekövetkezési valószínűségeiket és az általuk okozott kár mértékét – *helyesbítő* és *megelőző kontrollok* bevezetését célzó akciókat definiálunk, azok sorrendjének (prioritás) és kockázati mértékének (kategóriájának) meghatározása mellett (alacsony, közepes, magas).

A feltárt problémák kezelésére több alternatív megoldás is létezhet. A megoldási javaslatok megfogalmazása során figyelembe kell venni az EKF speciális helyzetét, és a lehető leggyorsabban, illetve legegyszerűbben kivitelezhető, illetve leginkább költség-hatékony megoldást célszerű javasolni.

2.5. Kontrollok implementálása, bevezetési akciók végrehajtása

A javasolt kontrollok a következők lehetnek:

a. Javító akciók: az egyszeri, a működés hiányosságait orvosló akciók
b. Megelőző intézkedések (preventív kontrollok): azok az akciók, amelyek végrehajtásával az egyes kockázatok bekövetkezési valószínűségét, illetve hatásuk mértékét lehet csökkenteni. Ezek:
    - Humán: emberi erőforrást érintő akciók (pl. oktatás, biztonsági tudatosság növelése, kiválasztás, stb.).
    - Adminisztratív: a működéshez kapcsolódó szabályzatok kidolgozása (biztonsági szabályzat, katasztrófa-elhárítási terv, stb.).
    - Fizikai: a fizikai környezet kialakítása (pl. betörésvédelem, beléptetés, stb.).
    - Logikai/technikai: az IT rendszerek beállításai, üzemeltetési gyakorlatuk (pl. azonosítók, jelszavak kezelése, naplózás, elemzések, stb.)

3. Az IT biztonsággal kapcsolatban vizsgálandó kategóriák, problémák

A helyzetfelmérési interjúkon elhangzott főbb megállapításokat, biztonsági problémákat, a helyszíni bejárások alkalmával észlelt hiányosságokat rögzíteni kell. Ezek pl. táblázatos formában összesíthetők.

Ezekhez kapcsolódóan megfogalmazásra kerülnek a problémák megoldására, az informatikai biztonsági rések megszüntetésére, a gyenge pontok megerősítésére vonatkozó javaslatok.

A javasolt akciók sürgősségi és kockázati mérőszámmal láthatók el a problémák prioritásának és kritikusságának függvényében.

A javaslatoknál figyelembe kell venni, hogy valamely biztonsági intézkedés hiánya nem feltétlenül jelent automatikus fenyegetettséget, illetve kockázatot; egy kontroll hiányát egy másik megléte kompenzálhatja, illetve egy meglévő kontroll részben (vagy akár teljesen is) át is veheti egy hiányzó kontroll helyét és szerepét.

3.1. Szervezeti és humán veszélyforrások és intézkedések

Szervezet

Kiválasztás

Munkakör

Képzettség

Elégedettség

Munkaviszony, hallgatói viszony megszűnése

Függőség

3.2. Adminisztratív biztonsági veszélyforrások és intézkedések

Tervezés

Minősítés

Szoftver beszerzés, módosítás, fejlesztés

Dokumentáció

Ellenőrzés

3.3. Fizikai biztonsági veszélyforrások és intézkedések

Lokációk

Kontroll

Természeti veszélyek

Áramellátás

Környezet

Megbízhatóság

3.4. Logikai biztonsági veszélyforrások és intézkedések

Jogosultságok

Jelszavak

Naplózás

Vírusok

Mentés, visszatöltés

Javasolt vizsgálati jegyzőkönyv-séma

Vizsgálati kategória	Az informatikai biztonsággal kapcsolatban vizsgált kategória.
Biztonsági probléma	A biztonsági probléma/ák megnevezése, esetleg a fontosabb pozitívumok kiemelése.
Biztonsági kockázat	A hiányosság, fenyegetés, veszélyforrás vagy sebezhetőség által okozott kockázat osztályba sorolása: Magas/Közepes/Alacsony.
Sürgősség	A beavatkozás javasolt gyorsasága: Kiemelten sürgős/Sürgős/Kevésbé sürgős.
Megoldási javaslat	A javasolt akció a megállapított hiányosság vagy biztonsági probléma kiküszöbölésére.

4. Az IT biztonsági helyzetértékelés összefoglalása

A legfontosabb megállapítások és javaslatok felsorolása.

AZ INFORMÁCIÓS VAGYON FELMÉRÉSE

„A" épület Bérügyi Csoport, I.emelet, 226 szoba

1. SZERVER INFORMÁCIÓS ŰRLAP

Megnevezés:	PLUTO/TÜSZ SZERVER
Leírás:	Novell környezeti alapú fájlszerver, gazdasági programok futtatására alkalmas környezet
Felelős:	Márföldi Endre, Kerecsendi András
Üzleti terület:	Gazdasági terület, informatikai üzemviteli menedzsment
Célja (felhasználás):	TÜSZ (Teljes Ügyviteli Szoftver) – gazdasági folyamatok nyomon követése, e-TÜSZ alkalmazás futtatása, leltározási folyamatok nyilvántartása
Tároló adathordozók:	2 db 80 Gb-os IDE HDD, szoftveres RAID 1-gyel
Működtetés helye:	A" épület Bérügyi Csoport, I.emelet, 226 szoba
Feldolgozási hely:	Bérügyi Csoport, Gazdasági Hivatal és az önálló egységek saját segítségével
Bizalmasság kárértéke:	Magas
Kárértékelés:	A szerveren tárolt adatok szerinti közvetett anyagi kár: az eszmei értéke kiemelkedő kárérték szempontjából. Napi mentés készül az adatokról, így maximum – sikertelen visszaállítás esetén – 8 munkaórányi adat veszhet el. Hardverelemek szerinti közvetlen anyagi kár: a csere illetve a javítás, valamint adatvisszaállítás költségei nem lépik túl a kárérték maximális összegét.
Megjegyzés:	Hamarosan grafikus felületre való áttérés várható, azonban ehhez szervercsere is szükséges

Szerver technikai amortizációja (százalék): 30 %

Adatvesztés nélküli rendelkezésre állás várható maximális ideje: 2010. július

Javasolt helyettesítő konfiguráció:

- 4 magos CPU (darabszáma bővíthető legyen),
- 8 GB RAM,
- 1 TB HDD,
- Windows Server 2008
- önálló szalagos egység a mentéshez.

2. ADATHORDOZÓ ŰRLAP

Megnevezés:	HDD
Felelős:	Márföldi Endre, Kerecsendi András
Típusa:	számítástechnikai eszköz
Leírás:	2 db 80 Gb-os IDE HDD, hardveres RAID 1-gyel,
Sértetlenség kárértéke:	Kiemelkedő
Üzleti terület:	Gazdasági terület;
Célja (felhasználás):	Gazdasági folyamatok, változások, mozgások adattárolása
Tárolás helye:	A" épület Bérügyi Csoport, I.emelet, 226 szoba
Tárolás módja:	Az adatok számítástechnikai eszközökön tárolódnak, amelyek tárolása megfelel a IK adattárolásra vonatkozó szabályainak (fizikai beléptetés, zárt hely, tűzbiztos tárolás). I/N Egyéb:
Attribútumok:	Eredeti példány □igen Hiteles □igen Történetiség □- Iktatott □- Archivált □igen Mentett □igen
Hitelesítés módja:	nincs
Mentés módja:	Napi mentés, minden nap hajnali 3 órakor, több helyre, több példányban.
Archiválás módja:	Az adatokat FTP-n keresztül átmozgatjuk, majd DAT kazettára is lementjük.
Elévülés/lejárat ideje:	A törvényi szabályozásnak megfelelően
Tárolt információk:	pénzügyi, valamint eszközadatok
Használó folyamatok:	csak gazdasági, és ahhoz köthető üzemviteli feladatokkal való munka
Alkalmazások:	Novell 6, TÜSZ
Kárértékelés:	A szerveren tárolt adatok szerinti közvetett anyagi kár: az eszmei értéke kiemelkedő kárérték szempontjából. Napi mentés készül az adatokról, így maximum – sikertelen visszaállítás esetén – 8 munkaórányi adat veszhet el.

Hardverelemek szerinti közvetlen anyagi kár:
a csere illetve a javítás, valamint adatvisszaállítás költségei nem lépik túl a kárérték maximális összegét.

Megjegyzés: -

Melléklet
(részletesebb kidolgozás kell: a közvetlen anyagi káron kívül több más szempontok is szóba jöhet, pl. közvetett anyagi kár, erkölcsi kár, bizalmassági kár, stb.)
Kérérték-kategóriák (pl. közvetlen anyagi kár szerint):

- Jelentéktelen: < 100.000 Ft
- Csekély: ≥ 100.000 Ft, < 1 mFt
- Közepes: ≥ 1 mFt, < 10 mFt
- Nagy: ≥ 10 mFt, < 100 mFt
- Kiemelkedő: ≥ 100 mFt

AZ INFORMÁCIÓS VAGYON FELMÉRÉSE

„A” épület szerverszoba, IV. emelet, 501 szoba

1. SZERVER INFORMÁCIÓS ŰRLAP

Megnevezés:	EKF BÉRÜGYI PROGRAM SZERVERE
Leírás:	WINDOWS 2003 szerver, bérprogramok futtatása
Felelős:	Márföldi Endre, Kerecsendi András
Üzleti terület:	Bérszámfejtési terület, informatikai üzemviteli menedzsment
Célja (felhasználás):	NEXON bérügyi folyamatok menedzsmentje;
Tároló adathordozók:	2 db 60Gb-os SCSI HDD, hardveres RAID 1-gyel
Működtetés helye:	Informatikai Központ szerverszobája
Feldolgozási hely:	Bérügyi Csoport és az önálló egységek saját segítségével
Bizalmasság kárértéke:	Kiemelkedő
Kárértékelés:	A szerveren tárolt adatok szerinti közvetett anyagi kár: az eszmei értéke kiemelkedő kárérték szempontjából. Napi mentés készül az adatokról, így maximum – sikertelen visszaállítás esetén – 8 munkaórányi adat veszhet el. Hardverelemek szerinti közvetlen anyagi kár: a csere illetve a javítás, valamint adatvisszaállítás költségei nem lépik túl a kárérték maximális összegét.

Megjegyzés:

Szerver technikai amortizációja (százalék): 45 %

Adatvesztés nélküli rendelkezésre állás várható maximális ideje: 2010. július

Javasolt helyettesítő konfiguráció:

- 4 magos CPU (darabszáma bővíthető legyen),
- 8 GB RAM,
- 1 TB HDD,
- Windows Server 2008
- önálló szalagos egység a mentéshez.

2. ADATHORDOZÓ ŰRLAP

Megnevezés:	HDD
Felelős:	Márföldi Endre, Kerecsendi András

Típusa:	számítástechnikai eszköz
Leírás:	2 db 60Gb-os SCSI HDD, hardveres RAID 1-gyel,
Sértetlenség kárértéke:	Kiemelkedő
Üzleti terület:	Gazdasági terület, bérszámfejtés;
Célja (felhasználás):	Bérszámfejtési adatok, folyamatok adattárolása;
Tárolás helye:	„A” épület szerverszoba
Tárolás módja:	Az adatok számítástechnikai eszközökön tárolódnak, amelyek tárolása megfelel a IK adattárolásra vonatkozó szabályainak (fizikai és logikai beléptetés, zárt hely, tűzbiztos tárolás). I/N Egyéb:
Attribútumok:	Eredeti példány □igen Hiteles □igen Történetiség □- Iktatott □- Archivált □igen Mentett □igen
Hitelesítés módja:	nincs
Mentés módja:	Napi mentés, minden nap hajnali 3 órakor, több helyre, több példányban.
Archiválás módja:	Az adatokat FTP-n keresztül átmozgatjuk, majd DVD lemezre és DAT kazettára is lementjük.
Elévülés/lejárat ideje:	A törvényi szabályozásnak megfelelően
Tárolt információk:	béradatok
Használó folyamatok:	bérszámfejtés
Alkalmazások:	Windows Server 2003, NEXON bérprogramb
Kárértékelés:	A szerveren tárolt adatok szerinti közvetett anyagi kár: az eszmei értéke kiemelkedő kárérték szempontjából. Napi mentés készül az adatokról, így maximum – sikertelen visszaállítás esetén – 8 munkaórányi adat veszhet el. Hardverelemek szerinti közvetlen anyagi kár: a csere illetve a javítás, valamint adatvisszaállítás költségei nem lépik túl a kárérték maximális összegét.

Megjegyzés: -

Melléklet
(részletesebb kidolgozás kell: a közvetlen anyagi káron kívül több más szempontok is szóba jöhet, pl. közvetett anyagi kár, erkölcsi kár, bizalmassági kár, stb.)

Kérérték-kategóriák (pl. közvetlen anyagi kár szerint):

- Jelentéktelen: < 100.000 Ft
- Csekély: ≥ 100.000 Ft, < 1 mFt
- Közepes: ≥ 1 mFt, < 10 mFt
- Nagy: ≥ 10 mFt, < 100 mFt
- Kiemelkedő: ≥ 100 mFt

AZ INFORMÁCIÓS VAGYON FELMÉRÉSE

„A” épület szerverszoba, IV. emelet, 501 szoba

1. SZERVER INFORMÁCIÓS ŰRLAP

Megnevezés:	EKF NEPTUN ADATBÁZIS szerver
Leírás:	WINDOWS 2008 szerver, Oracle futtatása
Felelős:	Márföldi Endre, Kerecsendi András
Üzleti terület:	Tanulmányi rendszer
Célja (felhasználás):	Tanulmányi rendszer adatbázisa
Tároló adathordozók:	4 db 140Gb-os SCSI HDD, hardveres RAID 1-gyel
Működtetés helye:	Informatikai Központ szerverszobája
Feldolgozási hely:	TIK
Bizalmasság kárértéke:	Kiemelkedő
Kárértékelés:	A szerveren tárolt adatok szerinti közvetett anyagi kár: az eszmei értéke kiemelkedő kárérték szempontjából. Napi mentés készül az adatokról, így maximum – sikertelen visszaállítás esetén – 8 munkaórányi adat veszhet el. Hardverelemek szerinti közvetlen anyagi kár: a csere illetve a javítás, valamint adatvisszaállítás költségei nem lépik túl a kárérték maximális összegét.
Megjegyzés:	

Szerver technikai amortizációja (százalék): 0 %

Adatvesztés nélküli rendelkezésre állás várható maximális ideje: 2014. július

Javasolt helyettesítő konfiguráció: jelenleg nem szükséges

.

2. ADATHORDOZÓ ŰRLAP

Megnevezés:	HDD
Felelős:	Márföldi Endre, Kerecsendi András
Típusa:	számítástechnikai eszköz
Leírás:	4 db 140Gb-os SCSI HDD, hardveres RAID 1-gyel

Sértetlenség kárértéke:	Kiemelkedő
Üzleti terület:	Tanulmányi rendszer
Célja (felhasználás):	Tanulmányi rendszer adatbázis
Tárolás helye:	„A” épület szerverszoba
Tárolás módja:	Az adatok számítástechnikai eszközökön tárolódnak, amelyek tárolása megfelel a IK adattárolásra vonatkozó szabályainak (fizikai és logikai beléptetés, zárt hely, tűzbiztos tárolás). I/N Egyéb:
Attribútumok:	Eredeti példány □igen Hiteles □igen Történetiség □- Iktatott □- Archivált □igen Mentett □igen
Hitelesítés módja:	nincs
Mentés módja:	Napi mentés, minden nap hajnali 3 órakor, több helyre, több példányban.
Archiválás módja:	Az adatokat FTP-n keresztül átmozgatjuk, majd DVD lemezre és DAT kazettára is lementjük.
Elévülés/lejárat ideje:	A törvényi szabályozásnak megfelelően
Tárolt információk:	tanulmányi adatok
Használó folyamatok:	Neptun rendszer
Alkalmazások:	Windows Server 2008, Oracle adatbázis-kezelő
Kárértékelés:	A szerveren tárolt adatok szerinti közvetett anyagi kár: az eszmei értéke kiemelkedő kárérték szempontjából. Napi mentés készül az adatokról, így maximum – sikertelen visszaállítás esetén – 8 munkaórányi adat veszhet el. Hardverelemek szerinti közvetlen anyagi kár: a csere illetve a javítás, valamint adatvisszaállítás költségei nem lépik túl a kárérték maximális összegét.
Megjegyzés:	-

Melléklet

(részletesebb kidolgozás kell: a közvetlen anyagi káron kívül több más szempontok is szóba jöhet, pl. közvetett anyagi kár, erkölcsi kár, bizalmassági kár, stb.)

Kérérték-kategóriák (pl. közvetlen anyagi kár szerint):

- Jelentéktelen: < 100.000 Ft
- Csekély: ≥ 100.000 Ft, < 1 mFt
- Közepes: ≥ 1 mFt, < 10 mFt
- Nagy: ≥ 10 mFt, < 100 mFt
- Kiemelkedő: ≥ 100 mFt