Tiszántúli Református Egyházkerület

4026 Debrecen, Kálvin tér 17.

INFORMATIKAI SZABÁLYZAT

Debrecen, 2015

1. Bevezetés

Jelen Informatikai adatvédelmi és adatkezelési szabályzatot a Tiszántúli Református Egyházkerület (továbbiakban: TTRE) . (a továbbiakban: Adatkezelő) fogadta el, vezette be és helyezte hatályba 2015. január 1. napjával, illetve tette munkaszervezetén belül kötelezően alkalmazandóvá az 2011. évi CXII. törvény
az információs önrendelkezési jogról és az információszabadságról történő megfelelés érdekében.

A szabályzat megalkotásának és kiadásának fontos további célja, hogy megismerésével és betartásával a szervezet alkalmazottai képesek legyenek a természetes személyek adatainak kezelését jogszerűen végezni.

A jelen szabályzat alkalmazója:

Tiszántúli Református Egyházkerült
Székhely: 4026 Debrecen, Kálvin tér 17.
Adószám: 19876182-2-09
Képviselők: Dr. Fekete Károly püspök, Dr. Adorján Gusztáv Tamás
Telefonszám: +36 52/514500
E-mail cím: tiszantul@reformatus.hu

Az Informatikai szabályzat által biztosítható:

a) A titok- és információ vagyon védelemre vonatkozó előírások betartása.
b) A személyiségi jogok kellő védelme.
c) Az üzemeltetett informatikai eszközök, hálózatok, stb. rendeltetésszerű használata és megfelelő üzemvitele.
d) Az üzembiztonságot szolgáló műszaki fenntartási és karbantartási teendők elvégzése.
e) A számítógépes feldolgozások és az eredményadatok további hasznosítása során az illetéktelen hozzáférésből és felhasználásból eredő károk megelőzése, illetve minimális mértékűre való csökkentése.
f) Az adatállományok formai és tartalmi helyességének és épségének megőrzése.
g) Az alkalmazott szoftverek sértetlenségének, megbízható működésének biztosítása.
h) Az adatállományok biztonságos mentése.
i) Annak rögzítése, hogy mi a szervezetek vezető beosztású és az informatikai feladatokat irányító dolgozóinak a feladata, felelőssége és a jogköre az informatikai biztonság tekintetében.
j) A jogosultság és a hozzáférés rendszerének dokumentált kialakítása.

A célok elérése érdekében a védelemnek működnie kell az egyes rendszerelemek fennállásának teljes ciklusa alatt — a megtervezéstől az alkalmazáson (üzemeltetésen) keresztül a felszámolásukig.

Az Informatikai Szabályzat az informatikai biztonsággal összefüggő szabályzásokat, ezek dokumentálását és az ellenőrzésének leírását, vagy ezek hivatkozásait tartalmazza.
Az Informatikai Szabályzat magában foglalja

a) az informatikai biztonság meghatározását, általános célkitűzéseit és tárgykörét, valamint a biztonság és a védelmi intézkedések fontosságát abban a mechanizmusban, amely az információ megosztását teszi lehetővé;
b) a vezetőség álláspontját, hogy miként támogatja az informatikai biztonság céljait és elveit;
c) az Informatikai rendszer elemeinek tervezését és új elemeinek bevezetését, üzemeltetését és használatát informatikai biztonság menedzselésének (Informatikai Biztonsági Felelős és informatikai szervezet) általános és sajátos felelősségi körei meghatározását, beleértve a jelentéskészítést minden biztonsági eseményről;

1.1 Személyi hatálya

Jelen szabályzat hatálya kiterjed a TTRE valamennyi munka- és felelősségi körében érintett dolgozójára, illetve a TTRE területén, vagy a TTRE adataival dolgozó szerződéses alvállalkozókra, illetve mindazokra, akik a TTRE -től informatikai szolgáltatásokat vesznek igénybe.

1.2 Tárgyi hatálya

Az informatikai szabályzat alkalmazása kiterjed az Informatikai rendszerben működtetett valamennyi hardver berendezésre, Szoftver elemre és ezek dokumentációira. (fejlesztési, szervezési, programozási, műszaki, üzemeltetési, biztonsági) és az Informatikai rendszerben feldolgozott adatállományok teljes körére.

2. Felelősségek, hatáskörök, elkötelezettségek az IT biztonság területén

2.1 Általános

A TTRE minden munkatársa, valamint minden a TTRE szerződésben lévő informatikai alvállalkozó és természetes személy felelős:

a) Informatikai szabályzat munkaterületére meghatározott előírásainak betartásáért és betartatásáért,

b) munkaterületén az adatbiztonság és a bizalmas adatok, információk megtartásáért, a nyilvánosságra hozatal megakadályozásáért.

A TTRE minden munkatársa köteles:

a) az Informatikai szabályzat dokumentumában előírt ellenőrzések és az auditok sikeres megvalósítását elősegíteni és támogatni;

b) tudomásul venni, hogy az Informatikai csoportvezető előzetes bejelentés nélkül ellenőrizheti az informatikai biztonsághoz kapcsolódó utasítások, szabályzatok betartását.

2.2 Informatikai csoportvezető

2.2.1 Feladata

a) az Informatikai rendszer Informatikai szabályzat megfelelő működtetése;

b) az Informatikai rendszer működtetéséhez szükséges valamennyi személyi és tárgyi erőforrás a szabályzatban definiált informatikai biztonsági elvárások figyelembe vétele alapján történő biztosítása;

2.3 Informatikai csoportvezető

2.3.1 Felelőssége

Az Informatikai csoportvezető felelősséggel tartozik az Informatikai rendszer működtetéséért.
Az Informatikai csoportvezető a biztonság szervezési szintű megvalósításáért, valamint támogatja a védelmi intézkedések meghatározását.

2.3.2 Jogosultsága

Az Informatikai csoportvezető jogosult

a) az Informatikai rendszer teljes körű ellenőrzésére;
b) az informatikai biztonságot érintő szabályzatok, utasítások és dokumentumok véleményezésére.

3. Az informatikai rendszer általános biztonsági alapelvei

a) A TTRE az általa kezelt adatok, valamint Informatikai rendszere tekintetében a felmerülő kockázatokkal arányos egyen szilárdságú védelmet alakít ki.

b) Az alkalmazott informatikai rendszerek és azok üzemeltetési rendje biztosítsák a rendszer és a rendszerben feldolgozandó adatok rendelkezésre állását, hitelességét, sértetlenségét és titkosságát azok teljes feldolgozási folyamatában.

c) A TTRE az információvédelem területén biztosítsa az informatikai rendszer gyártói ajánlásoknak és biztonsági követelményeknek történő megfelelését.

d) Az informatikai biztonsági megoldásokat úgy kell kialakítani, hogy azok rendszerek mindennapi alkalmazásának és üzemeltetésének hatékonyságát a lehető legkisebb mértékben befolyásolják.

e) Az informatikai rendszer alkalmazására és üzemeltetésére vonatkozó szervezeti és működési rendeket, nyilvántartási és tájékoztatási szabályokat, az informatika alkalmazásából eredő biztonsági kockázatok figyelembevételével úgy kell kialakítani, hogy a felelősségi körök és az egyértelmű személyes felelősségek meghatározhatók legyenek.

4. Felülvizsgálat és értékelés

Az Informatikai Biztonsági Felelős gondoskodik arról, hogy a szabályzatok felülvizsgálata minden jelentős változást követően megtörténjen (biztonsági esemény,

a szervezeti vagy műszaki infrastruktúra újabb sérülékenységei vagy változásai). Időszakos felülvizsgálatokat is be kell ütemezni a következőkre való tekintettel:

a) a szabályzat hatásossága a feljegyzett biztonsági események természete, száma és hatása alapján;

b) a technológiai, műszaki változások hatásai.

5. A vagyon osztályozása és ellenőrzése

5.1 A vagyoni felelősségre vonhatóság

5.1.1 Eszközvagyon leltár

A TTRE képes kell, hogy legyen azonosítani az informatikai eszközvagyonát és adatvagyonát (továbbiakban: vagyontárgy), és megállapítani ezek viszonylagos értékét és fontosságát. Erre az információra alapozva a TTRE a vagyon értékével és jelentőségével arányosan tudja megállapítani a védelmi szinteket. Leltárt kell készíteni minden olyan jelentős vagyontárgyról, amely valamelyik Informatikai rendszerrel kapcsolatos, és a leltárt karban kell tartani. Egyértelműen azonosítani kell valamennyi vagyontárgyat, meg kell állapítani és dokumentálni kell annak tulajdonjogát és biztonsági osztályát, valamint pillanatnyi elhelyezését.

5.1.2 Eszközök tulajdonosai

Az új munkavállalók belépésekor a munkavégzéshez szükséges eszközöket (számítógép, mobil telefon, egyéb mobileszközök) az állományi bizonylatban kerülnek felsorolásra és átadásra. Az eszköz átvételét a munkavállaló az aláírásával elismeri.
Az egyénhez nem rendelhető informatikai vagyontárgyakat a felhasználó szervezeti egységhez, mint csoporthoz kell hozzárendelni. A felelősség ezekben az esetekben a felhasználó szervezeti egység vezetőjéé.

5.1.3 Az eszközök elfogadható használata

Az informatikai eszközök használatának módját szabályozni kell (pl. csak hivatalos célokra) szem előtt tartva a biztonsági szempontokat.

a) A felhasználó köteles az eszközöket és a szoftvereket rendeltetésüknek megfelelően használni.
b) A felhasználó köteles a tőle elvárható gondossággal eljárni az eszközök használata során. Az eszközöket védeni köteles rongálás vagy szándékos károkozás ellen.
c) A felhasználó a rábízott eszközöket nem adhatja kölcsön harmadik személynek kockáztatva így az eszköz épségét, és az esetlegesen rajta lévő adatok biztonságát és sértetlenségét.
d) A felhasználó bármilyen hibát vagy sérülést észlel, azonnal jelentenie kell az informatikának.

e) A felhasználó a használatába adott eszközökön csak a munkavégzéséhez szükséges feladatokat végezheti, magán célokra nem használhatja azt.
f) Tilos az eszközök személyes haszonszerzés, illetve nem a TTRE érdekében történő használata.
g) Tilos a politikai vagy erkölcsi, vagy más törvénybe, vagy jó erkölcsbe ütköző anyagok készítése, tárolása, közlése, megjelenítése a TTRE eszközein.
h) A TTRE információ feldolgozó eszközeit a TTRE helyiségeiből csak külön engedéllyel szabad kivinni.
i) A TTRE információ feldolgozó rendszeréhez személyes információ feldolgozó eszközt csatlakoztatni csak külön engedéllyel szabad.

6. A személyzet biztonsága

6.1 Az alkalmazás alatt

6.1.1 Menedzsment felelősségek

A vezetőség felelőssége, hogy biztosítsák, hogy az alkalmazottak, illetve szerződő felek, vagy a TTRE egyéb jogviszony alapján munkát végzők:

a) megfelelő tájékoztatását az információ biztonsági feladataikról és felelősségükről mielőtt az érzékeny információkhoz vagy információs rendszerekhez hozzáférést biztosítanak számukra; a biztonsági irányelvekhez (szabályzatokhoz) hozzáférhessenek;
c) a Informatikai adatvédelmi és adatkezelési szabályzat betartásának fontosságával tisztában legyenek;
d) megfelelő tudatossági szintet érjenek el a biztonságra vonatkozóan;
e) a munkavégzéshez szükséges megfelelő jártasságuk és minősítésük legyen.

7.1.1 Informatikai biztonsági tudatosság, oktatás és tréning

A felhasználók, valamint a kijelölt külsős munkatársak számára az informatikai rendszer biztonságos használatával kapcsolatos rendszeres oktatást, tájékoztatást az informatikai csoportvezető végzi.

Oktatással elő kell segíteni, hogy a felhasználók felismerjék azokat a veszélyhelyzeteket, amelyek az intézménynek károkat okozhatnak (pl. vírusok terjesztése, adatvesztés, Szoftverek jogosulatlan használata vagy másolása stb.),

A külső munkatársak informatikai biztonsági oktatását a munkavégzés megkezdése előtt kell elvégezni.

7.1.2 Fegyelmi eljárások

A informatikai adatvédelmi és adatkezelési szabályzat megsértése esetén, az esetet ki kell vizsgálni. A kivizsgálást az informatikai csoportvezető végzi amennyiben szükséges az informatika munkatársainak bevonásával.

A vizsgálat eredményéről, a megtett intézkedésekről emlékeztetőt kell készíteni, a jegyző számára. Felelős: az informatikai csoportvezető.

Bűncselekmény elkövetése esetén büntetőjogi felelősség is fennáll.

Az alkalmazás megszűnése vagy megváltozása

7.1.3 A felelősségek megszűnése

Az alkalmazás befejezése után továbbra is érvényben maradó felelősségeket és kötelezettségeket az alkalmazott, szerződő fél vagy harmadik fél felhasználó szerződésében, vagy egyéb dokumentumban szerepeltetni kell. Ezért a munkavégző területi vezetője a felelős.

7.1.4 Az eszközök visszaszolgáltatása

Minden, használatra kiadott informatikai eszközt a jogviszony megszűnése előtt a vezetőnél le kell adni. Az eszközök visszavételét a vezető az eszköz átadási jegyzőkönyvön igazolja, e nélkül a dolgozó TTRE jogviszonyát nem lehet megszüntetni.

Szerződő fél végső teljesítés igazolása, amennyiben informatikai és/vagy kommunikációs eszközöket vett át a munka elvégzéséhez, csak a visszaszolgáltatási igazolás megléte esetén igazolható.

7.1.5 Hozzáférési jogok eltávolítása

A TTRE jogviszony megszűnésével az összes hozzáférési jogosultságot deaktiválni kell a területi vezető által közölt napon, a közléstől számított legrövidebb idő, de legfeljebb 1 napon belül.

Gondoskodni kell a felhasználó által készített, illetve használt elektronikus dokumentumok archiválásáról és az illetékes területi vezető részére való átadásról vagy törléséről.

Szerződéses munkavégző esetén a hozzáférési jogosultságokat csak a munkavégzés idejére szabad kiadni. A jogosultságok visszavonásának megtörténtét írásban, vagy emailben dokumentálni kell.

A felhasználó azonosítóját inaktívvá kell tenni, és az azonosítót egy éven belül újra kiadni tilos.

Az informatikai jogosultság nyilvántartást aktualizálni kell.

8. Fizikai és környezeti biztonság

8.1 Fizikai beléptetési óvintézkedések

A szerverszobába belépőknek a szerverszobában elhelyezett benntartózkodási naplóba magukat bejegyezni kötelesek. A szerverszobában illetékteleneknek tartózkodni tilos.

Az informatikai rendszer biztonságos működése számára a számítógépközpontban klimatizált légteret, szünetmentes tápellátást, tűzjelző és -oltó berendezést kell biztosítani.

A berendezéseket meg kell védeni a tápáramellátás, illetve más közmű szolgáltatások meghibásodásától és más villamos rendellenességektől. Olyan villamos tápáramellátást alkalmazni, amelyik megfelel a berendezésgyártó specifikációjának. A tápáramellátás folyamatosságát az alábbi megoldásokkal, illetve azok kombinációjával kell biztosítani:

8.2 Az irodák, a helyiségek és az eszközök biztonságba helyezése

A TTRE irodákkal, és az eszközök biztonságba helyezésével kapcsolatos szabályozások a következők.

Az alábbi védelmi intézkedéseket kell megvalósítani:

a) a kulcsfontosságú eszközöket úgy kell elhelyezni, hogy a nyilvánosság hozzáférését elkerüljük;

b) irodai berendezéseket és eszközöket, mint a fénymásolókat, faxokat, úgy kell elhelyezni, hogy a nyilvánosság hozzáférését elkerüljük;

c) az ajtókat és ablakokat, ha nincs a közelben felügyelő személyzet, zárva kell tartani. Az ablakok külső védelméről is gondoskodni kell, különösen a földszinten;

d) veszélyes vagy gyúlékony anyagokat biztonságosan kell tárolni a biztonsági körlettől, informatikai eszközöktől biztos távolságban;

e) a tartalék berendezéseket és a mentett adatokat tartalmazó adathordozókat olyan biztonságos távolságban kell elhelyezni, amellyel elkerülhető, hogy a központi telephely katasztrófája esetén kárt szenvedjenek.

Fentiek ellenőrzéséért felelős az Információ Biztonsági Felelős.

Külső és környezeti fenyegetések elleni védelem

Kockázatokkal arányos fizikai védelmet kell tervezni és alkalmazni a tűz, árvíz, földrengés, robbanás, polgári zavargás és más természeti vagy emberi jellegű károsodás ellen.

a) a veszélyes vagy éghető anyagokat a biztonsági területtől biztonságos távolságban kell tárolni;

b) megfelelő tűzoltó-berendezéseket és ezek megfelelő elhelyezését kell biztosítani.

8.3 A kábelezés biztonsága

A tápáramellátás kábelezését, valamint az adattovábbító és az informatikai szolgáltatások ellátásában használt távközló kábeleket meg kell védeni a zavaroktól és a sérülésektől.

Az információ-feldolgozó rendszerekhez csatlakozó energetikai és távközlési kábeleket, ahol lehetséges, a föld alatt kell vezetni, vagy megfelelő alternatív védelemmel kell ellátni.

A hálózati kábelezést meg kell védeni a jogosulatlan lehallgatástól vagy károsodástól, például külön védőcsövek alkalmazásával vagy a nyilvános hozzáférésű területen való vonalvezetés elkerülésével.

A zavarok elkerülése érdekében a kommunikációs kábeleket külön kell vezetni az erősáramú kábelektől.

A berendezések karbantartása

A berendezéseket a dokumentációjukban leírtaknak megfelelően kell kezelni és karbantartani, ezzel is biztosítva azok folyamatos rendelkezésre állását.
A berendezéseket a gyártó által ajánlott szervizidőszakok és -specifikációk szerint kell karbantartani.

A berendezéseken a javításokat és a szerviz-tevékenységeket kizárólag az arra feljogosított, megfelelő szakértelemmel rendelkező személyzet végezheti.

Minden feltételezett és tényleges meghibásodásról, valamint valamennyi megelőző és javító karbantartásról feljegyzést kell készíteni.

Megfelelő védelmi intézkedéseket kell életbe léptetni akkor, amikor berendezések karbantartásra házon kívülre kerülnek (lásd még a 9.2.6. szakaszt a törölt, a törölt és felülírt adatok vonatkozásában).

8.4 A berendezés házon kívüli biztonsága

A hordozható számítógépeket kézipoggyászban, és ahol lehet, utazás közben elrejtett módon kell szállítani.

A gyártók berendezés-védelmi utasításait mindenkor be kell tartani.

A mobil berendezések védelméről további információ található a 11.7.1. fejezetben.

Minden munkatársnak az elvárható gondossággal kell eljárnia a fenti esetekben. Fentiek felügyeletéért a területi vezetők és ellenőrzéséért az Informatikai Biztonsági Felelős a felelős.

8.5 A berendezés biztonságos újrahasznosítása vagy az azzal való biztonságos

rendelkezés

Berendezések gondatlan átengedése vagy ismételt használatba vétele az információ veszélyeztetéséhez vezethet. Az érzékeny információt tartalmazó tárolóeszközöket vagy fizikailag meg kell semmisíteni, vagy biztonságosan, helyreállíthatatlanul felül kell írni (pl. többszörös felülírásos törlés) az egyszerű, szokásos törlési művelet alkalmazása helyett.

A berendezések adatot tartalmazó valamennyi részegységét, a lemezegységeket ellenőrizni kell, hogy az érzékeny információt és a vásárolt szoftvereket arról eltávolították és felülírták, mielőtt mások rendelkezésére bocsátották volna.

Az érzékeny információt tartalmazó, de sérült tárolóeszközök tartalmának kritikussága alapján kell meghatározni, hogy az adott eszköz megsemmisítésre, vagy javításra kerüljön.

8.6 A tulajdon eltávolítása

Írásos engedély nélkül (állandó vagy eseti) berendezést, információt vagy szoftvert házon kívülre kivinni nem szabad.

Információ feldolgozó eszközök kivitele csak szállítólevéllel, valamint a szervezeti egység vezetőjének írásos engedélyével lehetséges.

Helyszíni ellenőrzéseket kell végezni annak érdekében, hogy a vagyontárgyak illetéktelen eltávolítását észre lehessen venni. A helyszíni ellenőrzések lehetőségéről mindenkit tájékoztatni kell.

9. Változáskezelés

Az informatikai rendszerben bármely változás csak ellenőrzött módon vezethető be, biztosítani kell, hogy a változások jóváhagyottak legyenek. ő

A változások nyilvántartásának tartalmaznia kell a változásokat engedélyező vezető személy nevét.

A szolgáltatás nyújtásában bekövetkező változtatásokat, illetve a szolgáltatással kapcsolatosan végbemenő változásokat kezelni kell. Szükség szerint változtatásokat kell végrehajtani, a szolgáltatással érintett rendszerek és kapcsolódó folyamatok

Védelem rosszindulatú szoftver ellen

9.1 A rosszindulatú kódok elleni óvintézkedések

Az informatikai rendszerben a vírus és egyéb programozott támadások megelőzése, kivédése érdekében, a vonatkozó kockázatokkal arányos, többszintű, rendszeresen frissített vírusvédelmi rendszert kell üzemeltetni. A szükséges frissítéseket rendszeres időközönként, szúrópróbaszerűen ellenőrizni kell.

A külső forrásból érkező adathordozókat, elektronikus leveleket felhasználásuk előtt vírusvédelmi szempontból ellenőrizni kell.

A vírusvédelemnek - többszintű vírusvédelmi rendszer működtetetése útján — az informatikai rendszer egész területén érvényesülnie kell.

Az informatikai rendszer vírusvédelmét többszintű szervereken és munkaállomásokon működtetett vírusvédelmi rendszerekkel kell biztosítani

A vírusellenőrző programok felügyelete a Vírusvédelmi Felelős feladata.

Az Informatikai rendszerben a vírusellenőrző programok rendelkezésre álló legfrissebb adatbázisa kell, hogy működjön. Az adatbázisok rendszeres frissítését automatikus letöltésekkel kell biztosítani.

Az informatikai rendszer berendezésein a vírusellenőrző program felhasználó általi kikapcsolása tilos. Ha a kikapcsolás rendkívüli esetben szükségessé válik, akkor ez kizárólag az Üzemeltetési Vezető jóváhagyásával hajtható végre. A végrehajtó kötelessége ilyenkor, hogy a vírusvédelmet a lehető legrövidebb időn belül visszakapcsolja. A vírusellenőrző program ki- és visszakapcsolását dokumentálni kell.

Az informatikai rendszerben a vírusfertőzés biztonsági eseménynek számít, ezért azt haladéktalanul az Informatikai Biztonsági Felelős felé jelenteni, majd kivizsgálni szükséges. Felelős: az illetékes felhasználó a jelentésért, a Vírusvédelmi felelős a kivizsgálásáért.

9.2 A mobil kódok elleni óvintézkedések

Mobil kódok az általában az internetről letölthető, és a helyi munkaállomáson - általában kifejezett telepítés nélkül - végrehajtódó állományok

A mobil kódok használata, futtatása csak külön engedéllyel lehetséges. A mobil kódot futtató eszközökön biztosítani kell, hogy a biztonsági beállítások megelőzzék a rosszindulatú mobil kódok futását. Biztosítani kell azt is, hogy nem engedélyezett mobil kódot ne lehessen futtatni.

9.3 Biztonsági mentés

A TTRE működésének biztosításához alkalmazott rendszereiről, valamint az ügyvitel szempontjából kritikus informatikai eszközökön elhelyezett adatokról rendszeres mentést kell készíteni, a napló adatokat archiválni szükséges.

A TTRE tevékenysége ellátásához rendelkeznie kell olyan eszközzel, amely lehetővé teszi a rendszerek és adatok olyan mentési rend végrehajtásával végzett biztonsági mentését (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amely az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszi.

A TTRE adatait kettő adatközpontban (Fűvészkert 4., Egyetemi templom) tárolja ezekről az adatokról az átellenes adatközpontba napi mentést kell készíteni.

Az Informatikai Biztonsági Felelős rendszeresen (minimum 1 havonta) ellenőrzi a mentések elkészültét, valamint a visszaállítási tesztek megtörténtét.

9.4 Hálózatmenedzselés

9.4.1 A hálózati óvintézkedések

A TTRE fizikailag független illetve virtuális hálózatainak esetében az egyes hálózatok tekintetében egységes biztonsági szabályrendszert kell alkalmazni.

A LAN, WAN hálózati forgalomban — továbbiakban: hálózati forgalom - a hálózaton továbbított adatok felfedésének kockázatával, azok minősítésének megfelelő arányos biztonsági megoldásokat kell alkalmazni.

A kommunikációs rendszereket úgy kell kialakítani, hogy biztosítsák az adatátvitel bizalmasságát, rendelkezésre állását, hitelességét, sértetlenségét.

A külvilág felől jelentkező fenyegetettség elfogadható szintre történő csökkentése érdekében a hálózati forgalom folyamatos szűrésére preventív biztonsági megoldásokat kell alkalmazni.

A hálózat elemeit, a hálózati forgalmat rendszeresen ellenőrizni kell annak érdekében, hogy a hálózati forgalom illetéktelen monitorozása felfedésre kerüljön.

Minden informatikai rendszerhez csatlakoztatott vagy attól függetlenül használt munkaállomásról pontos és naprakész nyilvántartást kell vezetni.

Az informatikai rendszerben a felhasználók számára az informatikai erőforrások használatát hozzáférés-menedzsment útján kell szabályozni. Minden Felhasználó csak a munkaköri feladatai ellátásához szükséges erőforrásokhoz férhessen hozzá.

A helyi hálózat számítógépközponton kívüli diszkrét és aktív elemeit lehetőség szerint zárható, biztonsági szempontból feltörésvédett szekrényben kell elhelyezni.

A hálózati szolgáltatások biztonsága

A biztonsággal összefüggő paraméterek és minősített adatok csak és kizárólag megfelelő kriptográfiai protokoll alkalmazásával továbbíthatók.

Az informatikai rendszer a külvilág felé szigorúan szabályozott módon, a kezelt adatok minősítésének megfelelő, hitelesítési és forgalom ellenőrzési eljárások betartásával kapcsolódhat.

A nyilvános és a magánhálózatokon elérhető szolgáltatásokat igénybe vevő szervezeti egységeknek gondoskodniuk kell arról, hogy el legyenek látva valamennyi igénybe vett szolgáltatás biztonsági jellemzőnek egyértelmű leírásával. A szükséges biztonsági beállításokhoz az üzemeltetés munkatársai nyújtanak segítséget

9.5 Az adathordozók kezelése és biztonsága

9.5.1 A hordozható számítógépes adathordozók menedzselése

Az olyan eltávolítható számítógépi adathordozók menedzselésére, mint a szalagok, lemezek, memóriakártyák, megfelelő eljárásokat kell kialakítani.

Bármely újra használható adathordozó tartalmát visszaállíthatatlan módon törölni kell, ha arra már nincs szükség és az adathordozót a szervezeti egységtől elviszik.

Minden adathordozót biztonságosan kell tárolni az adathordozón levő adatok besorolása, valamint a gyártói előírások szerint

Adathordozónak számítanak a következő eszközök:

a) USB kulcs

b) CD lemez
c) DVD lemez
d) Szalag
e) Mikrofilm
f) Notebook
g) Hordozható Winchester
h) Asztali számítógép
i) Szerver
j) Okostelefon

Biztosítani kell, hogy az adathordozók kezelése a vonatkozó iratkezelési szabályok szellemében, a tartalmazott adatok szempontjából egyenértékű papír dokumentumokkal azonos módon történjék. Az adathordozók kezelése során az adathordozó által tartalmazott adatok minősítésének megfelelően kell eljárni.

Minden adathordozót biztonságos és védett környezetben kell tárolni a gyártói előírások szerint

9.5.2 Rendelkezés az adathordozók felett

Az adathordozókat, ha már nincsenek rendszeres használatban, biztonságos és védett módon kell elhelyezni. Az adathordozók nem megfelelő elhelyezése érzékeny információk kívülálló személyekhez való kiszivárogtatására vezethet.

Az érzékeny információt tartalmazó adathordozókat biztonságos és védett módon kell tárolni vagy megsemmisíteni.

9.5.3 Az információkezelési eljárások

Az információt kezelő eljárásokat azért kell kialakítani, hogy az információt a jogosulatlan nyilvánosságra kerüléstől és a visszaéléstől megóvjuk. Az eljárásokat úgy kell kialakítani, hogy azok a dokumentumra, számítástechnikai rendszerre, hálózatra, mobil számítástechnikára, mobil távközlő rendszerre, levélre, hangpostára, általában a hangátvitelre, multimédiára, postai szolgáltatásokra, faxgépek használatára és más érzékeny tételekre, például csekklapokra, számlákra vonatkozó osztályozással összhangban legyenek.

A mentési adathordozókat a mentési rendre vonatkozó Mentési és Archiválási Szabályzat szerint kell jelöléssel ellátni.

A papír alapú dokumentumok címkézését keletkezésük helyén kell elvégezni.

9.6 Információcsere

9.6.1 Információcserére vonatkozó szabályzat és eljárások

Az információt veszélyeztetheti a faxok, telefonok, fénymásolók használatakor a gondosság, szabályzat vagy eljárások hiánya.

Az élőszóban és telekommunikációs eszközökön történő információ közlés veszélyes pontját jelentik a mindkét fél halló, illetve látótávolságán belül tartózkodó illetéktelen

személyek, valamint a faxkészülékek szándékos vagy véletlen félreprogramozása, illetve a faxok véletlen rossz számra való elküldése.

Az információ védelmének érdekében a következő irányelveket kell követni:

a) Bizalmas megbeszélések nem történhetnek nyilvános helyen, nyitott irodákban vagy vékony falú helyiségekben.
b) Telefonon való bizalmas adatközlést kerülni kell.
c) Telefonbeszélgetés során szem előtt kell tartani a lehallgatás lehetőségét. Veszélyt jelenthetnek a telefon fogadó oldalán tartózkodó személyek is.
d) Üzenetrögzítőn nem hagyható védett adatot tartalmazó üzenetek.
e) Fax küldése előtt ellenőrizni kell a címzett faxszámát, valamint, ha lehetséges a készülék kijelzőjén a tárcsázni kívánt számot.
f) Fax küldését követően, amennyiben az érzékeny információt tartalmaz lehetőség szerint meg kell győződni, hogy azt tényleg a címzett kapta meg.

9.6.2 Az elektronikus üzenetek biztonsága

A TTRE fontosnak tartja munkatársai hatékony belső és külsőkommunikációját, ezért munkatársai számára elektronikus levelezési lehetőséget biztosít.

Az informatikai rendszer levelezőrendszerében az üzenetek és a levelek a személyes elektronikus postaládákon keresztül kerülnek továbbításra.

A TTRE az elektronikus levelek tartalmát vírusellenőrzésnek veti alá.

A TTRE jogosult az elektronikus levelezőrendszerében továbbított üzenet, levél vagy fax tartalmát, az üzenet, levél vagy fax feladójának vagy címzettjének kiszolgáltatása nélkül, a hatóság számára az ide vonatkozó jogszabályi megalapozottság esetén kérésre - átadni. A TTRE a hatóság kérését minden esetben bizalmasan kezeli.

9.6.3 Az elektronikus irodai rendszerek biztonsága

A TTRE irodáiban elhelyezett fénymásolók és faxok minden munkavállaló számára hozzáférhetők, korlátozás nélkül használhatók. A munkavállalók felelőssége ügyelni az eszközökben másolt, továbbított, nyomtatott papír alapú dokumentumok kezelésére. Használat után minden esetben ellenőrizni kell, hogy nem maradtak-e dokumentumok az eszközökben, kiadó tálcáin, illetve környezetében. Az őrizetlenül hagyott dokumentumokat lehetőség szerint el kell juttatni azok tulajdonosának.

Az elektronikus irodai rendszerek használata, során biztonsági szempontból fegyelembe kell venni az alábbiakat.

a) az irodai rendszerekben az információ sérülékenységét, például a telefonhívások és a konferenciabeszélgetés rögzítését, a hívások titkosságát, a faxüzenetek tárolását, levelek felbontását és a levelek szétosztását;
b) az érzékeny információ egyes kategóriái továbbításának kizárását, ha a rendszer nem nyújt elegendő védelmet;
c) az eszköz által tárolt információ érzékenységét.

9.4 Nyilvánosan hozzáférhető rendszerek

A TTRE nyilvánosan hozzáférhető informatikai rendszere a ttre.hu weboldala.

9.5 Rendszergazda és operátor naplók

Az informatikai rendszerben végrehajtott műveleteket, objektumokhoz történő hozzáférést a kockázatokkal arányosan kell naplózni mind alkalmazás, mind operációs rendszer, mind adatbázis rendszer szinten. Az alkalmazott naplózásnak és a kapcsolódó kiegészítő adminisztrációnak olyan részletezettségűnek kell lennie, hogy abból az esemény érdemi értékelése elvégezhető, az egyértelmű személyes felelősség megállapítható legyen.

Az informatikai rendszer naplózási rendszerében biztosítani kell az informatikai rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosítását.

Gondoskodni kell olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza.

A fentiek szerinti naplózás rendszeres és érdemi értékeléséről gondoskodni kell.

Minden naplózást lehetőség szerint úgy kell beállítani, hogy a felhasználó éles adathoz naplózási lehetőségek megkerülésével ne férhessen hozzá.

9.6 Hiba naplózás

Az informatikai rendszer biztonsági és egyéb meghibásodását vagy rendellenes működését szóban vagy e-mail-en keresztül kell bejelenteni az üzemeltetőnek. Felelős: a meghibásodást vagy rendellenes működést észlelő személy.

A bejelentett hibákat a hibát fogadó személy a hiba naplóba rögzíteni köteles.

A hiba kijavítását követően a hiba elhárításáról a hibát bejelentő személyt értesíteni kell. Felelős: az elhárítást végző, illetve külső támogató cég közreműködése esetén az azt felügyelő üzemeltető munkatárs.

10. Hozzáférés és ellenőrzés

10.1 A hozzáférés—ellenőrzés követelményei

A felhasználó részére az informatikai rendszerbe belépést engedélyezni csak és kizárólag abban az esetben szabad, ha a felhasználó valamilyen módon azonosítja magát.

Az informatikai rendszer erőforrásait és felhasználóinak hozzáférési jogait egységes elvek alapján kell meghatározni és kiosztani.

Az informatikai rendszer felhasználóinak hozzáférési jogait központilag nyilván kell tartani. A központi jogosultság-nyilvántartási rendszer tartalmazza a jogosultság kezeléshez kapcsolódó mindazon adatokat, amelyekből egyértelműen megállapítható, hogy kinek, milyen rendszerhez, milyen jogosultságai vannak.

A nem egyértelműen egy természetes vagy jogi személyhez kötött felhasználói azonosítók (technikai vagy service accountok) esetén a jelszavakra a négy szem elv alkalmazását kell előírni.

Az informatikai rendszerben haladéktalanul meg kell szüntetni/fel kell függeszteni azon személyek hozzáférési jogait, akiknek jogviszonya a TTRE megszűnt.

10.1.2 A hozzáférés—ellenőrzés szabályzata

Minden Felhasználó részére az általa használt szoftverben saját névre szóló nevesített felhasználó-azonosítót kell beállítani, amivel a felhasználó jogkörénél fogva alkalmassá válik a szoftver használatára.

A felhasználó-azonosítók kiosztásakor alkalmazandó névkonvenciót, az azonosítók kiosztásának és karbantartásának a rendjét az Informatikai csoportvezető határozza meg.

10.2 A felhasználói hozzáférés menedzselése

A felhasználói jogosultságok kezelésének részletes szabályait a Jogosultságkezelési szabályzat tartalmazza

Az informatikai rendszerben minden felhasználó csak és kizárólag munkakörének maradéktalan elvégzéséhez szükséges hozzáférési jogosultságokkal rendelkezhet, figyelembe véve az összeférhetetlenségeket. Kivételt képezhet, ha az informatikai rendszer működtetése ezt nem teszi lehetővé, ebben az esetben a kockázatnövekedést egyéb ellenőrző intézkedésekkel kell ellensúlyozni.

Az éles rendszerben hibajavítás, fejlesztés, technológiai vagy egyéb változások miatt szükséges átmeneti jogosultságokat csak a szükséges időtartamra szabad kiadni.

A jogviszony időleges vagy végleges megszűnése esetében a munkavállaló jogosultságainak visszavonását a megadott megszűnési dátum figyelembevételével, az informatika a megszűnés napján hajtja végre.

10.2.1 A felhasználó nyilvántartásba vétele

Minden több felhasználós informatikai rendszerhez és szolgáltatáshoz a hozzáférési jog megadásakor a felhasználó jogosultságait nyilvántartásba kell venni.

A helyettesítést lehetőség szerint úgy kell megoldani, hogy olyan személy vegye át a feladatokat, akinek a helyettesítettel megegyező (vagy hasonló, de a munka végzéséhez elegendő) jogosultsága van az adott rendszerhez, s így a saját jogán végzi a feladatokat. A más felhasználó nevével (felhasználói fiókjával) történő munkavégzés nem megengedett.

10.2.2 A felhasználói jelszó gondozása

A jelszó a felhasználó azonosságát igazolja, hogy hozzáférhessen az informatikai rendszerhez vagy egy szolgáltatáshoz. A jelszavakat szabályos jelszógondozási folyamattal kell kísérni:

a) gondoskodni kell arról, hogy azoknál a rendszereknél, ahol a felhasználóktól megkívánják saját jelszavaik karbantartását, cseréjét, ott első alkalommal egy biztonságos ideiglenes jelszóval

legyenek ellátva, de azt kényszerüljenek azonnal lecserélni. Ideiglenes jelszavakkal a jelszavukat elfelejtő felhasználókat csak akkor szabad ellátni, ha már a felhasználó azonosítása megtörtént;

b) a felhasználók, nyilatkozzanak, hogy titokban tartják személyes jelszavaikat és a csoportjelszavakat kizárólag a csoporttagokra korlátozzák;

c) a felhasználóknak az ideiglenes jelszavakat csak biztonságos környezetben szabad átadni. Az ideiglenes jelszavak használatát a szükséges minimumra kell csökkenteni. Ideiglenes jelszavakat harmadik személy bevonásával vagy elektronikus levélüzenetben továbbítani tilos. A felhasználók nyugtázzák a jelszavak átvételét. Sohasem szabad jelszót számítógépen védetlen formában tárolni.

10.2.3 A felhasználói hozzáférési jogok felülvizsgálata

Az adatokhoz és az informatikai rendszerekhez való hozzáférés hatékony ellenőrzését azzal kell fenntartani, hogy a felhasználók hozzáférési jogait időről időre felül kell vizsgálni:

a) a felhasználók hozzáférési jogait rendszeresen felül kell vizsgálni általánosan legalább évente, vagy az informatikai alkalmazásokban bekövetkező jelentős változást követően;

b) a külön kiváltsággal rendelkező hozzáférési jogokra szóló felhatalmazásokat félévente kell felülvizsgálni.

10.3 A felhasználó felelősségi köre

10.3.1 Jelszóhasználat

A jelszó eszközt jelent a felhasználó azonosságának igazolására és arra, hogy az informatikai rendszer elemeihez, illetve szolgáltatásaihoz hozzáférési jogai érvényesüljenek. A felhasználóknak a jelszavak kiválasztásában és használatában az alábbiakban felsorolt biztonsági gyakorlatot kell követniük:

a) a jelszavait titokban kell tartania;

b) kerülje a jelszavak papírra rögzítését;

c) mindannyiszor és mindakkor cseréljen jelszót, ha bármi jel arra mutat, hogy a rendszer vagy a jelszó veszélyeztetve van, illetve a rendszer a cserét megköveteli;

d) válasszon minőségi jelszót,

e) jelszavait időről időre cserélje, és kerülje el mind a korábbi jelszavak ismételt használatát, mind a már használt jelszavak ciklikus átrendezését;

f) cserélje le ideiglenes jelszavait az első bejelentkezés alkalmával;

g) ne írja be jelszavait automatikus bejelentkezési folyamatokba, amelyet a számítógép, makrók vagy funkcionális billentyűk tárolnak,

h) felhasználó a TTRE informatikai hálózatán vagy annak bármely informatikai rendszerében azonosításra használt jelszavát külső

informatikai rendszerekben nem használhatja, köteles eltérő jelszavakat alkalmaznia.

Felelős: minden informatikai rendszer felhasználó.

10.3.2 Felügyeletlen felhasználói berendezés

A felhasználóknak gondoskodniuk kell arról, hogy a felügyeletlen berendezések kellő védelemmel rendelkezzenek. Az irodákban telepített berendezések, mint a munkaállomások, külön védelmet igényelnek a jogosulatlan hozzáféréssel szemben, amennyiben hosszabb időre felügyelet nélkül maradnak. Amennyiben ez megoldható, a védelemnek automatikusnak kell lennie.

A felhasználókat kötelezni kell arra, hogy

a) az aktív folyamatokat zárják le, ha a munka befejeződött és jelentkezzenek ki, vagy zárolják a munkaállomást, mely zárolást csak jelszóval lehet feloldani;

b) amikor a munkafolyamatokat befejezték, jelentkezzenek ki (nem elegendő ilyenkor a PC vagy munkaállomás egyszerű kikapcsolása);

c) a PC-t, vagy a munkaállomást, ha nincsen használatban, a jogosulatlan használattal szemben tegyék biztonságossá úgy, hogy vagy kijelentkeznek és kikapcsolják, vagy zárolják, mely zárolást csak jelszóval lehet feloldani.

10.4.1 A hálózati szolgáltatások használatának szabályzata

Az informatikai rendszerben jogosultságrendszer működtetése útján kell gondoskodni arról, hogy az informatikai rendszerben tárolt programokhoz, adatállományokhoz, adatokhoz kizárólag ellenőrzött és dokumentált módon lehessen csak hozzáférni, és az illetéktelen hozzáférés, az adatolvasás, az adatmegsemmisítés, az adathamisítás megakadályozható legyen.

Az Alkalmazásokban a felhasználói jogosultságok egyedi vagy szerepkör szinten történő megkülönböztetését kell előírni és azt nyilván kell tartani.

Egy hálózati szolgáltatáshoz hozzáférési jogot az a munkatárs kaphat:

a) akinek munkavégzéséhez az adott szolgáltatás használata szükséges;

b) aki rendelkezik az adott szolgáltatás biztonságos használatához szükséges szakmai, és információbiztonsági ismeretekkel;

c) és biztonsági vagy egyéb okból (pl. összeférhetetlenség) nem esik korlátozás alá;

10.4.2 A felhasználó hitelesítése külső hozzáférés esetén

A TTRE informatikai rendszerének távolról történő elérése VPN kapcsolattal lehetséges, melyhez külön vezetői engedély szükséges.

10.4.3 A berendezések azonosítása a hálózaton

Az automatikus felkapcsolódás lehetősége eshetőséget adhat jogosulatlan hozzáférésre alkalmazásokhoz is. Ezért a TTRE számítógéprendszerére eszközök csatlakoztatását minden esetben engedélyezni kell. Az informatikai rendszert lehetőség szerint úgy kell beállítani, hogy a nem engedélyezett eszközök ne kapcsolódhassanak a rendszerre.

10.4.4 Távdiagnosztikát végző csatlakozópont védelme

Távdiagnosztikát végző hálózati csatlakozópontok (portok) hozzáférését ellenőrizni kell. Igen sok számítógépet és távközló rendszert telepítenek úgy, hogy távdiagnosztikai képességeket is beállítanak a fenntartással foglalkozó mérnökök támogatására. Ha az ilyen távdiagnosztikát végző csatlakozópont védtelen, lehetőséget ad jogosulatlan hozzáférésre. Éppen ezért az ilyet védeni kell, olyan eljárással, amely szavatolni képes, hogy csak ellenőrzötten lehessen hozzáférni.

10.4.5 Hálózatdarabolás

Az informatikai hálózatok túlnyúlnak egyes szervezeti egységeken, sokszor kiterjednek a szervezetek fizikai határain túlra is. Az integrált feladatok szükségessé teszik, hogy egy rendszerhez különböző szervezeti egységek, illetve szervezetek férjenek hozzá, illetve az egyes rendszerek összekapcsolását. Az ilyen kapcsolatok fokozhatják az informatikai rendszerekhez történő hozzáférések kockázatát, így meg kell teremteni a védelmet más szervezetek, vagy szervezeti egységek felhasználóitól.

A hálózatot, biztonságának megteremtése és ellenőrzése érdekében, szükség szerint különböző logikai hálózati tartományokra kell felbontani.

10.5 Hozzáférés—ellenőrzés az operációs rendszeren

Az operációs rendszer szintjén elérhető biztonsági eszközöket arra kell használni, hogy korlátozzuk a hozzáférést a számítógép erőforrásokhoz.

Ezek az eszközök a következő képességekkel rendelkezzenek:

a) képesség az egyes jogosult felhasználók azonosságának, és szükség esetén munkaállomásának vagy telephelyének az azonosítására és igazolására;

b) képesség a sikeres és a sikertelen rendszer hozzáférések rögzítésére;

c) képesség a hitelesítés ellátására alkalmas eszközzel, és ha jelszógondozó rendszert alkalmaznak, akkor ez szavatolja a minőségi jelszavak használatát.

10.5.1 Biztonságos bejelentkezési eljárások

Biztonságos bejelentkezési folyamattal kell lehetővé tenni a hozzáférést az informatikai szolgáltatásokhoz. Valamely számítógép—rendszerhez a belépési eljárást úgy kell kialakítani, hogy a jogosulatlan hozzáférés esélyét a minimálisra csökkentsük. A beléptető eljárásnak éppen ezért a rendszerről csak a lehető legkevesebb információt szabad közreadnia, hogy elkerülhessük, hogy a jogosulatlan felhasználót segítse.

Ahol a rendszer lehetővé teszi

a) a rendszer a belépés előtt a lehető legkevesebb információt szolgáltassa a technológiáról;
b) sikertelen belépés esetén a rendszer nem jelölheti meg, hogy a megadott adatok mely része hibás;
c) limitálni kell a sikertelen belépések számát és a belépési folyamat maximális idejét;
d) limitálni kell a sikertelen belépések számát és a belépési folyamat maximális számát.

10.5.2 A felhasználó azonosítása és hitelesítése

Minden felhasználót - a műszaki személyzetet is beleértve - kizárólagos személyi használatra egyedi azonosítóval (felhasználói ID-vel) kell ellátni, hogy azt követően bármely tevékenység nyomon követhető legyen, egészen az azért felelős személyig bezárólag.

A felhasználói ID-k nem mutathatják semmi jelét a felhasználó kiváltságainak.

Az informatikai rendszerekhez való hozzáférés csak a felhasználói azonosító megadásával legyen lehetséges.

A felhasználó hitelesítésére az azonosító mellett jelszavakat kell használni. Ahol a kezelt adatok érzékenysége megkívánja, a rendszert úgy kell kialakítani, hogy az alkalmazáshoz való hozzáféréshez is a felhasználónak felhasználói névvel és jelszóval azonosítania kell magát.

A felhasználói azonosítók beállításáért az Informatikai csoportvezető felel

10.5.3 A rendszer segédprogramjainak használata

A legtöbb számítógéprendszer rendelkezik egy vagy több olyan segédprogrammal, amely képes a rendszer- és alkalmazásvezérlések hatástalanítására. Lényeges, hogy ezek használata korlátozott és szigorúan ellenőrzött legyen.

10.5.4 Az alkalmazás és információ-hozzáférés ellenőrzése

Biztonságtechnikai eszközöket úgy kell alkalmazni, hogy az alkalmazásokon belüli hozzáféréseket korlátozzuk. A logikai hozzáférést a szoftverhez és az információhoz a jogosult felhasználókra kell korlátozni.

Az alkalmazások

a) ellenőrizzék a felhasználói hozzáférést az információhoz és az alkalmazás funkcióihoz;
b) nyújtsanak védelmet az illetéktelen hozzáférés ellen valamennyi olyan operációs rendszerbéli és segédszoftver számára, amelyek képesek a rendszer vagy az alkalmazási vezérlések hatástalanítására;

c) kerüljék el más, olyan rendszerek biztonsági veszélyeztetését, amelyekkel az adott rendszer osztozik valamely informatikai erőforrás használatában;

d) legyenek képesek arra, hogy csak az arra megnevezett, felhatalmazott személyeknek vagy felhasználói csoportoknak vagy a tulajdonosnak tegyék lehetővé a hozzáférést az információhoz.

10.5.5 Az információhoz való hozzáférés korlátozása

Az alkalmazások felhasználóit, a műszaki támogató személyzetet is beleértve, előre meghatározott módon a Jogosultságkezelési szabályzat szerint kell ellátni hozzáféréssel mind az informatikai infrastruktúra, mind az alkalmazások funkcióihoz.

A következő óvintézkedéseket kell alkalmazni a hozzáférés korlátozás megvalósítására:

a) menük alkalmazását az alkalmazási rendszer funkcióihoz való hozzáférés ellenőrzésére;

b) a felhasználói ismeretek korlátozását a felhasználói dokumentumok megfelelő szerkesztésével azon informatikai funkciók és alkalmazási rendszerbéli funkciók terén, amelyekhez hozzáférésére nincsenek feljogosítva;

c) a felhasználók hozzáférési jogainak szabályozását, írás, olvasás, törlés tekintetében;

10.5.6 Az érzékeny (sérülékeny) rendszer elszigetelése

10.6 A mobil számítástechnika és a távmunka

10.6.1 Mobil számítástechnika és telekommunikáció

Mobil számítástechnikai eszközök—laptop és mobil telefon — használata esetén gondoskodni kell az információ veszélyeztetésének elkerüléséről.

Mobil számítástechnikai eszközök közterületeken, konferenciatermekben és más védetlen körzetben, a TTRE saját telephelyén kívüli használatakor fokozottan figyelni kell a biztonságra, arra, hogy az adatokhoz, információkhoz más jogosulatlan személyek (a közelben levő személyek) ne férjenek hozzá.

Megfelelő védelemmel kell ellátni a mobil eszközöket arra az esetre is, amikor azokat hálózatba kapcsolva használjuk. Az érzékeny információhoz a távoli hozzáférés, ha azt mobil számítástechnikai eszközökkel nyilvános hálózaton keresztül érjük el, csak sikeres azonosítás és a feljogosítás után történhessen.

A mobil számítástechnikai eszközt fizikailag is védeni kell a lopás ellen, különösen akkor, ha például gépkocsiban vagy más szállítóeszközön, hotelszobában, konferencia teremben és tanácskozó helyen hagyjuk. Berendezés, amely fontos, érzékeny és/vagy kritikus információt hordoz nem hagyható felügyelet nélkül, és ahol lehetséges azt fizikailag is el kell zárni, vagy azon a berendezés biztonsága érdekében különleges zárat kell alkalmazni.

11. Rendszer beszerzések, fejlesztések és azok karbantartása

11.1 A biztonsági követelmények elemzése és meghatározása

Az alkalmazások fejlesztése során kialakított rendszerek, rendszerelemek dokumentáltsága olyan részletezettségű kell, hogy legyen, hogy a TTRE azt a fejlesztő nélkül is képes legyen üzemeltetni, szükség esetén tovább fejleszteni.

Az informatikai rendszer hardver elemeinek fejlesztetése során kialakított dokumentációnak olyan részletezettségűnek kell lennie, hogy a TTRE azt a fejlesztő/szállító nélkül is képes legyen üzemeltetni (lehetőség szerint).

Fejlesztés / tervezés

Az operációs, az alap- és az alkalmazás rendszerek biztonsági funkcionalitását a rendszer által kezelt adatok besorolásának megfelelően kell kialakítani.

Az alkalmazások specifikálása során meg kell határozni a rendszerbe beépítendő biztonsági és ellenőrzési kritériumokat, valamint az adatok jóváhagyásának eljárásrendjét. Az alkalmazások adatainak kezeléséhez a felhasználók részére megfelelő felületet kell specifikálni.

Tesztelés

Az alkalmazások éles üzemi környezetbe történőtelepítésüket megelőzően az éles üzemi környezettől független tesztkörnyezetben a szállítóktól független, dokumentált tesztelésnek kell alávetni.

Tesztelés céljára a mentett, illetve archivált „éles" adatok felhasználását el kell kerülni. Ha ez nem valósítható meg, akkor az adatok titkosságát oly módon kell biztosítani, hogy az feleljen meg a jogszabályokban meghatározott adat- és titokvédelmi követelményeknek.

11.2 Kriptográfiai óvintézkedések

Az informatikai rendszer által kezelt adatokat - különös tekintettel a jogszabályokban meghatározott minősítésükre, az alkalmazott informatikai technológiára - az általuk megjelenített kockázatokkal arányos kódolási eljárásokkal kell védeni.

Az informatikai rendszer által tárolt felhasználóneveket, jelszavakat és hozzáférési listákat biztonsági besorolásuknak megfelelően, kriptográfiai eljárással kell védeni az illetéktelen felfedéstől.

11.3 A kriptográfiai óvintézkedések használatának szabályzata

A kriptográfiai megoldások alkalmaságára vonatkozó döntéshozatal egy szélesebb folyamat része kell, hogy legyen, amelyben felmérik a kockázatokat és meghatározzák a szükséges óvintézkedéseket.

11.4.1 A rendszerállományok/-fájlok biztonsága

Az informatikai eszközökre csak és kizárólag jogtiszta szoftvereket szabad telepíteni és üzemeltetni. A telepített szoftverekről és licenceikről nyilvántartást kell vezetni. A

telepítéshez szükséges minden adathordozót, dokumentációt, eszközt lehetőség szerint két példányban kell megőrizni, eltérő helyen.

11.4.2 Licencnyilvántartás

Minden az informatikai rendszerre és munkaállomásra telepített rendszerszoftver és alapszoftver jogtisztaságát igazoló licencről pontos és naprakész nyilvántartást kell vezetni.

Ajánlott a rendszerszoftver és alapszoftver elemek pontos és naprakész leltárba vételét automatikus eljárással végezni.

11.4.3 Rendszervizsgálati adatok védelme

A teszt adatokat védeni és ellenőrizni kell. Mind a rendszervizsgálatok, mind az átvételi vizsgálatok többnyire jelentős mennyiségű olyan adatot igényelnek, amelyek eléggé közel állnak az éles adatokhoz. Az éles adatbázis használatát kerülni kell. Ha mégis ilyen információ kerül használatra, akkor az adatokat meg kell fosztani személyes jellegüktől, illetve megfelelő módosításokat kell végrehajtani ahhoz, hogy eltérjenek az éles adatoktól.

11.5.1 Az operációs rendszer változásainak műszaki felülvizsgálata

Időről időre szükség lehet arra, hogy az operációs rendszert lecseréljük, hogy egy újonnan leszállított szoftverváltozatot vagy egy javítást telepítsünk.

Az operációs rendszer változtatása esetén az alábbi szempontokat kell figyelembe venni:

a) Az alkalmazási rendszereket át kell tekinteni, és tesztelni kell annak érdekében, hogy szavatolni lehessen, hogy a változás az üzemeltetésre és a biztonságra nincsen negatív hatással.

b) Az ügymenet folyamatosságára vonatkozó tervekben amennyiben szükséges, a megfelelő változtatásokat át kell vezetni.

c) Amennyiben a változtatás (javítócsomag) nem befolyásolja hátrányosan az alkalmazások működését, a tesztelt javítócsomagot a legrövidebb időn belül telepíteni kell.

d) Az operációs rendszert úgy kell a rendszergazdának beállítani, hogy automatikusan ne kínálja fel a rendszer javítócsomagjának letöltését és/vagy telepítését. A javítócsomagot a felhasználók semmiképpen nem telepíthetik a munkaállomásokon.

11.5.2 A szoftvercsomagok változtatási korlátozása

A szoftvercsomagok nem frissítésként vagy verzióváltásként végrehajtott módosítását lehetőség szerint el kell kerülni. Amennyire csak lehetséges és a gyakorlatban az kivitelezhető, a szállító által adott szoftvercsomagot módosítás nélkül kell használni.

11.5.3 Információ kiszivárogtatás

Az információ kiszivárgását minden lehető eszközzel meg kell előzni. A megelőzés érdekében az alábbi szempontokat kell alkalmazni:

a) programokat csak tiszta forrásból szabad beszerezni;

b) csak bevizsgált, tesztelt terméket szabad használni;

c) minden forráskódot át kell vizsgálni használatba vétel előtt;

d) kulcsfontosságú rendszereken csak megbízható munkatársak dolgozzanak;

e) a munkatársak tevékenységének biztonsági ellenőrzésére a TTRE fenntartja a jogot.

A teszt rendszerben is történjen vírusellenőrzés.

11.6.1 A technikai sérülékenységek ellenőrzése

A használt információ feldolgozó rendszerek sebezhetőségére vonatkozó időszerű információkat, rendszeresen be kell szerezni. A sérülékenységek elleni védelem eszközeként az előzetesen megvizsgált frissítések minél előbb történő telepítését el kell végezni. (Patch-menedzsment). A frissítéseket ahol lehetséges központilag kell letölteni és telepíteni.

12. Informatikai biztonsági incidens kezelés

12.1 Jelentés az informatikai biztonsági eseményekről és gyengeségekről

12.1.1 Jelentés az informatikai biztonsági eseményekről

Az informatikai rendszer felhasználóitól meg kell követelni, hogy jelentsék a rendszerekben vagy a szolgáltatásokban minden felismert vagy feltételezett biztonsági eseményt, a rendellenestől eltérő működést. Ezeket haladéktalanul jelenteni kell vagy saját vezetőknek, vagy az üzemeltetőnek.

Az informatikai rendszer minden üzemzavarát, elemeinek minden meghibásodását hibanaplóba kell bejegyezni.

A bejelentést fogadónak legalább a következőket kell feljegyeznie a bejelentett eseményekről: a bejelentés ideje, a bejelentő neve, az esemény rövid leírása, feltételezett oka, az elhárítás résztvevője, az elhárítás kezdete, az elhárításához megtett intézkedés, az elhárítás vége.

12.1.2 Jelentés a biztonsági sérülékenységekről

Az informatikai rendszer felhasználóitól meg kell követelni, hogy jelentsék a rendszerek vagy a szolgáltatások minden felismert vagy feltételezett biztonsági gyengeségét vagy fenyegetettségét. Ezeket haladéktalanul jelenteni kell vagy saját vezetőiknek, vagy az üzemeltetőnek. A felhasználók a feltételezett gyengeséget semmilyen körülmények között se próbálják maguk megszüntetni.

12.2 A biztonsági eseményekre és incidensekre adott válasz és fejlesztés

12.2.1 Felelősségek és eljárások

A biztonsági események kezelésének felelősségeit és eljárásait úgy kell megállapítani, hogy a biztonsági eseményekre gyorsan, hatékonyan és rendben meg lehessen tenni a válaszlépéseket.

A következő védelmi intézkedéseket kell végrehajtani:

a napló állományokat és hasonló bizonyítékokat össze kell gyűjteni

Okulás a biztonsági eseményekből

Az ismétlődő és jelentős hatású biztonsági eseményeket rendszeresen elemezni, értékelni kell és ezek alapján kiegészítő és továbbfejlesztett védelmi intézkedéseket kell bevezetni vagy az informatikai adatvédelmi és adatkezelési szabályzatot felülvizsgálati folyamatában, illetve a képzési tervben figyelembe venni a későbbi előfordulások gyakorisága, kára és költségei korlátozására.

Bizonyítékok gyűjtése

Az informatikai biztonsági óvintézkedések kialakításakor törekedni kell arra, hogy az informatikai biztonság esetleges sérülése esetén a TTRE kellő bizonyítékkal rendelkezzen ahhoz, hogy indokolt esetben a bizonyíték támogasson egy intézkedést egy személy vagy más szervezet ellen.
Számítógép-adathordozón rögzített bizonyíték esetében a hordozható adathordozók, valamint a háttértárolón és a központi tárolón talált információ másolatait meg kell őrizni és rendelkezésre állásáról gondoskodni kell. Felelős az Informatikai Biztonsági Felelős.

A másolási folyamat során valamennyi tevékenységről naplófeljegyzést kell elkészíteni és tanú jelenléte szükséges. A napló és az adathordozó egy-egy példányát biztonságosan meg kell őrizni.

13. Megfelelőség

13.1 Megfelelés a jogi követelményeknek

13.1.1 A hatályos jog megállapítása

Minden vonatkozó törvényes, szabályozói vagy szerződéses követelményt részletesen meg kell határozni és megvizsgálni azok hatását az információs rendszerekre. A szervezeti egység vezetők felelősek a szabályozók betartatásáért.

13.1.2 Adatvédelem és a személyes információ védelme

Az informatikai adatvédelmi és adatkezelési szabályzat célja, hogy a TTRE működésében biztosítsa az adatok az információs önrendelkezési jogról az információszabadságról szóló 2011. évi CXII. törvényben meghatározott védelmét, s az adatbiztonság követelményeinek érvényesülését.

A rendszerek vizsgálatát — biztonsági osztályba sorolását - a 2013. L. törvény alapján kell elvégezni, valamint minden jelentős, az informatikai rendszert érintő változás esetén felül kell vizsgálni.

14. Hatályba lépés

A jelen szabályzat hatályba lépésének dátuma: 2015. január 1.

A Tiszántúli Református Egyházkerület Elnöksége nevében ellenjegyzem:

Dr. Fekete Károly
püspök