EKR 10. számú melléklet

18. Informatikai és biztonsági szabályzat[83]

Előszó

Mai világunkban egyre fontosabb szerepe van a számítógépeknek az azokat hálózatba kötő telekommunikációs rendszereknek. Az élet különböző területein ma már elképzelhetetlen a számítógép és az Internet használata nélkül boldogulni. Az állami, az oktatási és a gazdasági szféra munkavégzése egyaránt a számítógépek használatán alapul, így a számítógépes rendszerektől való függés egyre nagyobb és nagyobb lesz. A termelés, irányítás, oktatás által keletkezett információk, adatok nagy része már nemcsak papír alapon, hanem nagyrészt informatikai rendszerekben tárolódik. A világhálózat, az Internet terjedésével a kommunikáció és a világban való tájékozódás módja is megváltozik. Ebben az új világban az információ valódi értékké vált és annak védelme immáron elengedhetetlen. De nemcsak az adatot, információt, hanem magát a számítógépes rendszert is védeni szükséges, hiszen ezek támogatása nélkül könnyen megbénulhat a számítógépek által át meg átszőtt életünk.

Az informatikai biztonság, mint kedvező állapot elérése érdekében védelmi intézkedéseket kell alkalmaznunk. Ezeknek az intézkedéseknek át kell fogniuk az informatikai rendszer teljes életciklusát (létesítés, használat, változtatás, megszüntetés), és a védelemre fordított összeg arányban kell, hogy álljon az információ vagy a rendszer sérüléséből okozható kárral. Az informatikai rendszer védelme ki kell, hogy terjedjen a fizikai, a logikai, a humánpolitikai védelem területére, valamint speciális eszközök és eljárások használatára.

Ezt a védelmet nehezíti, hogy a számítógépes rendszerek bonyolultsági foka egyre nő. Manapság a legjobb szakemberek is nehéz helyzetben vannak, hiszen ebből a bonyolultságból adódóan nem ismerhetik részleteibe menően a pontos működési mechanizmusokat, így rendkívül nehéz arról meggyőződniük, hogy egy rendszer tényleg úgy működik-e, ahogy kellene, valóban biztonságos-e vagy sem. Egy átlagos felhasználó (egy irodai dolgozó, akinek kezében a számítástechnikai rendszer és szoftver nem cél, hanem csak használati eszköz), még ennyire sem ismeri a számítógépet (ugyanúgy ahogy a mikrohullámú sütő vagy televízió működését sem ismeri pontosan, csak használatának módját). Nehezen tudja eldönteni, hogy egy adott rendszert használva mennyire van kiszolgáltatva a számítógépen keresztül rosszindulatú embertársainak. Az előbbi példában ehhez nyújt segítséget a használati utasítás, amiből megtudhatja mindenki, hogy az elvárt funkcionalitás érdekében mit kell tennie, valamint a saját és környezete biztosságát hogyan tudja megóvni. Ilyen használati utasítás a számítástechnikai rendszerekhez az Informatikai Biztonsági Szabályzat, mely segít a helyes és biztonságos használat elsajátításában.

Ezen felül a rendszer folyamatos működésére nézve az egyes természeti tényezők (tűz, víz, villámcsapás, …) és a hardver meghibásodások is komoly veszélyt jelentenek, az adatok megsemmisülése mindennapos veszély. Ez a bizonytalanság bizalmatlanságot okoz, és a számítógépes rendszerek terjedését tekintve jelentős negatív hatása van.

Az Informatikai és biztonsági szabályzat törvényi háttere

2012. évi C. törvény (Btk.)

A törvény a hatályos Büntető Törvénykönyvet tartalmazza. A Büntető Törvénykönyvbe új vétségek és bűncselekmények kerültek be, mégpedig a következők:

- „Információs rendszer felhasználásával elkövetett csalás”
- „Tiltott adatszerzés”
- „Információs rendszer vagy adat megsértése” és
- „Információs rendszer védelmét biztosító technikai intézkedés kijátszása”.

A fenti kategóriák a Btk. 375. §, 422. §, 423. § illetve 424. paragrafusában találhatók.

A 375. § szerint három évig terjedő szabadságvesztéssel büntetendő, „aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz.” Ugyanennek súlyosabban minősülő eseteit a törvény nagyon szigorúan bünteti, egyes esetekben a büntetés mértéke megegyezik az emberölés alapesetének büntetésével.

[83] Elfogadta a Szenátus 2017. május 18-án kelt, 31/2017. (05.18.) sz. határozatával.

A 422. § (1) bekezdés b) – d) pontjai szerint a törvény bünteti, ha valaki „személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából
b) más lakásában, egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy rögzíti,
c) más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,
d) elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti,
bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.". Ugyanígy büntetendő az is, aki az ilyen módon „megismert személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot továbbít vagy felhasznál." Ugyanennek súlyosabban minősülő és egy évtől öt évig terjedő szabadságvesztéssel büntetendő változata, ha mindezt „hivatalos eljárás színlelésével, üzletszerűen, bűnszövetségben vagy jelentős érdeksérelmet okozva" követi el valaki.

A 423. paragrafus szerint két évig terjedő szabadságvesztéssel büntetendő, aki „információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad." Három évig terjedő szabadságvesztéssel büntetendő aki
„a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy
b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz."
A törvény még szigorúbb büntetéseket szab ki ez utóbbi két bűncselekmény minősített eseteire (pl. ha az jelentős számú információs rendszert érint, vagy közérdekű üzem ellen követik el), egyes esetekben a büntetés mértéke megegyezik az emberölés alapesetének büntetésével.

Ha valaki a fenti három „bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő
a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve
b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja," két évig terjedő szabadságvesztéssel büntethető.

Mentesül azonban a büntetés alól az, aki tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását még azelőtt, hogy a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntető ügyekben eljáró hatóság tudomására jutott volna.

A fenti bűncselekményekkel kapcsolatban:

„adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja."

„jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító."

2011. évi CXII. törvény (Info. tv.)

„7. § (1) Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.
(2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
(3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
(4) A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.
(5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja
a) a jogosulatlan adatbevitel megakadályozását;
b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;

d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.
(6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek."

2015. évi CCXXII. törvény

A 2015-ben elfogadott törvény az elektronikus ügyintézés és a bizalmi szolgáltatások jogi szabályozásának alapjait teremti meg.

2001. évi CVIII. törvény

A törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szól, több esetben módosították rendelkezéseit. A törvény összhangban van- egyebek között – az Európai Parlament és a Tanács 2000/31/EK jelű, 2000. június 8-i, azonos témájú irányelvével.

Szabályzat

1. Hálózathasználati szabályzat

1.1. Bevezetés

A Tan Kapuja Buddhista Főiskola hálózata jelenleg egy publikus hálózathoz kapcsolódik:

UPC HUNGARY

A szabályzat A Tan Kapuja Buddhista Főiskola Informatikai Biztonsági Szabályzatának többi rendelkezésével együttesen alkalmazandó, a szabályzat által nem tárgyalt kérdésekben a Magyarország hatályos törvényei az irányadók.

1.2. A szabályzat hatálya

Jelen szabályzat mindenkire nézve kötelező, aki használja A Tan Kapuja Buddhista Főiskola számítógép-hálózatát, annak berendezéseit (későbbiekben felhasználók). Az előbbieknek megfelelően a szabályzat személyi hatálya kiterjed A Tan Kapuja Buddhista Főiskola összes hallgatójára és dolgozójára, aki oktatási, kutatási, tudományos vagy az intézmény adminisztrációs feladataihoz A Tan Kapuja Buddhista Főiskola számítógép-hálózatát használja. Ha az intézmény harmadik félnek is lehetőséget biztosít hálózatának használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

1.3. A hálózat használatának szabályai

A Tan Kapuja Buddhista Főiskola hálózata nem használható az alábbi tevékenységekre:
a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése);
profitszerzést célzó, direkt üzleti célú tevékenység és reklám;
a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. levélbombák, hálózati játékok, kéretlen reklámok);
a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások – akár tesztelés céljából történő – túlzott mértékben való szisztematikus próbálgatása (pl. TCP port scan);
a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;

másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok közzététele);
hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

1.4. Felelősök

Felelősöket kell kinevezni, akik kontrollálják a hálózat egyes részeinek, szolgáltatásainak működését, rendeltetésszerű és szabályos használatát, valamint felelnek a biztonsági előírások betartásáért és betartatásáért. A felelősöket a rektor jelöli ki.

1.5. A felhasználók kötelességei

A felhasználók kötelessége a szabályzat megismerése és az abban foglaltak betartása, valamint együttműködni a hálózat üzemeltetőivel a szabályzat betartatása érdekében.

A felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználó azonosítóval kerül végrehajtásra.

1.6. A felhasználók jogai

Minden Főiskolai diáknak joga van a diák felhasználói fiókhoz, saját levelezéshez (e-mail címhez), web és news szolgáltatáshoz.
A felhasználónak joga van az internethez való hozzáféréshez. A Főiskola ezt a számítógép-teremben teszi lehetővé.
A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetői tiszteletben tartják, ettől eltérni csak a törvény által meghatározott esetekben lehet.
A rendszer technikai problémáiról (tervezett vagy rendkívüli eseményekről) tájékoztatni kell a felhasználókat.
A felhasználók számára elérhető módon közzé kell tenni a felhasználókra vonatkozó szabályok érvényes változatát.

1.7. Szankciók

A Szabályzat megsértésének gyanúja esetén az esetet ki kell vizsgálni, és a kijelölt felelősnek meg kell tennie a szükséges intézkedéseket, amelyre a következők az irányadók:
A Szabályzat előírásainak nem ismerete nem mentesít a következmények vállalásának kötelességétől.
A Szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni.
A Szabályzatnak egy figyelmeztetést követő ismételt megsértése szándékos elkövetésnek minősül.
A Szabályzat szándékos megsértése esetén az elkövető a hálózat használatából ideiglenesen vagy véglegesen kizárható, és az eset súlyosságától függően fegyelmi eljárás folytatható le ellene.
A szándékos elkövető köteles megtéríteni az általa okozott károkat a Polgári Törvénykönyv előírásai szerint.
Ha az elkövetett cselekedet kimeríti valamely hatályos magyar törvény tényállását, akkor a felelősnek kötelessége megtenni a megfelelő törvényi lépéseket.

2. Jelszókezelési szabályzat

2.1. Bevezetés

A jelszó a hozzáférés-kezelés alapvető eszköze, így az informatikai biztonság fontos része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszó fontosságával és a nem megfelelő jelszókezelés következményeivel, mert egy rosszul megválasztott, könnyen kitalálható jelszó nemcsak a jelszó tulajdonosára, hanem A Tan Kapuja Buddhista Főiskola informatikai rendszerére is negatív következményekkel járhat. A jelszavaknak két nagy csoportját különböztethetjük meg a következők alapján: adminisztrátori vagy egyszerű felhasználói jogú azonosítót véd a jelszó, a szabályozás ennek függvényében eltérhet, az adminisztrátori jelszavakra mindig a szigorúbb szabályok érvényesek.

2.2. A szabályzat hatálya

Jelen szabályzat mindenkire érvényes, aki A Tan Kapuja Buddhista Főiskola hálózatának bármely részéhez jelszó használatát igénylő hozzáféréssel rendelkezik.

2.3. Alapelvek

Nem szabad könnyen kitalálható jelszavakat választani! (A helyes jelszóválasztáshoz a 2.4-es fejezet ad segítséget.)
A jelszavakat mindenképp titokban kell tartani! (A jelszavak védelméről a 2.5-ös fejezetben található útmutató.)
Az induló jelszót az első bejelentkezéskor meg kell változtatni.
A jelszavakat rendszeres időközönként cserélni kell (adminisztrátori jelszó esetén 3 havonta ajánlott, egyéb esetben félévente).
Új jelszónak nem szabad az utolsó 5 régi közül egyiket sem megadni.
Ha a felhasználónak gyanúja támad, hogy jelszava kompromittálódhatott, azonnal meg kell változtatnia.
5 sikertelen próbálkozás után a felhasználói fiók zárolandó.
A jelszavakat nem szabad kódolatlanul tárolni.
Azon személyek, akik különböző rendszerekhez, illetve több felhasználói azonosítóval is rendelkeznek, a különböző rendszerekhez, azonosítókhoz különböző jelszavakat kell használniuk.
Ahol lehetséges, a jelszavakra vonatkozó alapszabályokat (jelszóhossz, jelszócsere, előző jelszavak megadásának tilalma) az adott informatikai rendszer segítségével ki kell kényszeríteni.

2.4. Helyes jelszóválasztás

Nem szabad könnyen kitalálható, személyre jellemző jelszavakat használni (pl. személyes adatok, családtagok, barátok neve, házi kedvenc neve…).
A jelszónak legalább 7 karakter hosszúnak kell lennie.
Nem szabad sorozatokat használni (pl. abcdefg, 7654321, asdfghj).
Kerülni kell a szótári szavak használatát (ezek egy számjeggyel kiegészített változatai sem biztonságosak).
A jelszó tartalmazzon kis- és nagybetűket, lehetőleg számokat és speciális karaktereket is.
A nemzeti billentyűzet állíthatósága miatt nem javasolt az ékezetes karakterek, az Y, a Z és a 0 (nulla) használata.
A jelszónak könnyen megjegyezhetőnek kell lennie. Könnyen megjegyezhető erős jelszavak például a jelmondat alapú betűszavak. Választunk egy kedvenc mondatot (szólást vagy idézetet akár), pl.: „Ki itt belépsz, hagyj fel minden reménnyel!”, majd ennek kezdőbetűiből összeállítunk egy betűszót: „kibhfmr”. Ezt utána variálhatjuk nagybetűkkel, számokkal, jelekkel, pl.: „kiB3hfmR-”, és kész az erős jelszó, amit később mégse lesz nehéz felidézni.
Végül pedig: Ne használjuk a példákban felsorolt jelszavakat!

2.5. Jelszóvédelem

A jelszót titokban kell tartani, másokkal azt nem szabad megosztani (családtagokkal, barátokkal sem). A legerősebb jelszó sem ér semmit, ha azt könnyen elérhető helyen tartjuk, vagy könnyen megszerezhető. Különösképpen figyelni kell az alábbiakra:
A jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni.
A jelszót se a feljebbvalóknak, se a rendszergazdáknak, adminisztrátoroknak nem szabad elárulni, ha kifejezetten kérik ezt, akkor sem.
Tilos közös jelszavakat használni (még családtagokkal, barátokkal sem szabad).
A jelszót nem szabad leírni, és elérhető helyen tárolni (irodában, táskában…).
A jelszót nem szabad semmilyen számítógépes rendszeren titkosítás nélkül (pl. egyszerű szövegfájlban) tárolni.
A jelszót nem szabad telefonon vagy e-mail-ben továbbítani.
Ne utaljunk a jelszó tartalmára (pl. „a kedvenc együttesem neve”).
Ne használjuk a programok jelszó megjegyző funkcióját.
A jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.
Ha a jelszó kompromittálódott, vagy erre utaló jeleket lehet észlelni, azonnal meg kell változtatni a jelszót, és értesíteni kell a rendszergazdát.
Cseréljük jelszavunkat legalább félévente (adminisztrátori jelszavaknál az ajánlott periódus 3 hónap). A jelszavak véletlen támadásoknak is áldozatul eshetnek, ezért fontos a rendszeres jelszócsere.

3. Vírusvédelmi szabályzat

3.1. Bevezetés

A számítógépes vírusok a számítógépen tárolt adatok és programok kártevői. A vírus a megfertőzött program futása közben másolja, többszörözi önmagát. Rendszerbe kerülésük történhet fertőzött lemeztől történő rend-

szerindítási kísérlet (bootvírusok), egy fertőzött program elindítása (fájlvírusok), egy vírusos makrókat tartalmazó dokumentum megnyitása (makrovírusok), Internet használat közben (etikailag nem javasolt tartalmak látogatása) vagy e-mail-ben csatolt állományként terjedő makró- illetve script vírusok, férgek megnyitásának eredményeként. A vírusok gépről gépre terjednek, többnyire észrevehetetlenek, amíg nem aktivizálódnak. Ekkor azonban nagy kárt okozhatnak pótolhatatlan adatok megsemmisítésével, a rendszer bénításával, bizonyos esetekben hardveres károkozással. A víruskeresők, vírusirtók használata elengedhetetlen, de ezek is csak a már ismert vírusok ellen jelentenek igazi védelmet.

Ez a szabályzat az előbbiekben felsorolt káros hatások megelőzésére, és a vírusfertőzés esetén elvégzendő teendők leírására szolgál.

3.2. A szabályzat hatálya

A vírusvédelmi szabályzat minden a Főiskola hálózatába kötött személyi számítógépre, pda-ra és szerverre vonatkozik.

3.3. Vírusfertőzés gyanús helyzetek

Sok jele lehet vírus jelenlétének, azonban ezek nagy része normál tevékenység eredményeként is előállhat. Mivel a vírusok írói általában igyekeznek elkerülni a feltűnő viselkedést, a felhasználó nem feltétlenül találkozik az alább felsorolt – vírusfertőzésre utaló – jelenségekkel:

A víruskereső program névvel azonosított vírust jelez. A lehető legerősebb vírusjegy.

Fájl másolása esetén az újonnan keletkezett és az eredeti példány hossza eltérő. Nagyon erős vírusjegy.

Szokatlan és váratlan képernyő tevékenység (szokatlan üzenetek, ablakok megjelenése). Erős vírusjegy.

Szokatlan számítógép- vagy programviselkedés (pl. programok maguktól elindulnak). Általánosan erős vírusjegy. Ha az operációs rendszer újraindítása után is fennáll, erős vírusjegynek tekinthető.

A rendszer működése többszöri újraindítás után is egyértelműen lassabb a megszokottnál. Átlagosan erős vírusjegy. Helytelen rendszerkonfiguráció is okozhatja.

3.4. Vírusvédelmi teendők

Az alábbi utasítások betartása erősen ajánlott a vírusfertőzések megelőzése, illetve azok kockázatának csökkentése érdekében:

Vírusvédelmi szoftvert kell használni. Biztosítani kell a szerverek, a munkaállomások és a pda-k vírusvédelmét. Ehhez A Tan Kapuja Buddhista Főiskola számára 22 felhasználói licencet biztosít a Panda Online Security. Ezek szabadon felhasználhatók minden Főiskolai számítógép védelmére.

A vírusvédelmi programnak rezidens módban kell futnia, így az minden egyes rendszerindításkor aktivizálódik, és állandó háttérvédelmet biztosít. A felhasználóknak nem szabad kikapcsolni ezt a védelmet.

Ne fusson egyszerre két vírusölő program.

Kéthetente minden gépen teljes vírusellenőrzést kell végrehajtani (a vírusvédelmi szoftver támogatja az időzített keresési funkciót).

A vírusvédelmi program vírusdefiníciós adatbázisát a lehető leggyakrabban frissíteni kell. Ha erre lehetőség van, az automatikus frissítést kell választani, így az új elemek rögtön megjelenésük után felkerülhetnek a rendszerre.

Idegen helyről származó adattárolókon (floppy, cd, dvd, pen-drive, HDD) használat előtt vírusellenőrzést kell végezni.

Soha nem szabad ismeretlen vagy gyanús helyről fájlokat letölteni.

A Ms-Office csomag programjainál, ahol lehet, be kell állítani a makrók jelenlétének kijelzése funkciót. Idegen állományokat csak makrók futtatása nélkül opcióval szabad megnyitni.

Ismeretlen, megbízhatatlan forrásból származó furcsa, gyakran vicces e-mail-ek csatolt fájljait nem szabad megnyitni, azonnal törölni kell őket. Az e-mailben küldött vírusok, férgek rendszeresen operálnak valamilyen különös megjegyzéssel a levelek tárgy bejegyzésében.

A fontos adatokról és a rendszerkonfigurációról készüljön archiválás.

3.5. Teendők vírusfertőzés esetén

Tájékoztatni kell a vírusvédelemért felelős személyt (számítástechnika tanárt, rendszergazdát,) a fertőzésről vagy annak gyanújáról.

A számítógépet újra kell indítani egy előkészített, vírusmentes, a használt operációs rendszert és a vírusvédelmi program legfrissebb változatát tartalmazó lemezről. Ha ez nem lehetséges, akkor védett módban kell újraindítani a gépet csak a legszükségesebb szolgáltatásokkal (lehetőleg hálózati kapcsolat nélkül).

A vírusvédelmi szoftvert elindítjuk, és megszüntetjük a vírusfertőzést. Ez történhet elsődlegesen a fertőzött állomány javításával (a vírus eltávolítása), ha erre lehetőség van, egyébként a fertőzött állomány törlésével. Ez utóbbi esetben ügyelni kell arra, hogy nem rendszerállományról van-e szó.
A víruskeresést addig kell végezni, amíg el nem éri a rendszerfelelős, hogy a víruskereső program úgy fusson végig az összes állományon, hogy fertőzött állományt már nem talál.
Ezek után a rendszer újraindítható a szokott módon.

4. Távoli elérés szabályzata

4.1. Bevezetés

A szabályzat célja, hogy irányt mutasson A Tan Kapuja Buddhista Főiskola belső hálózatához távoli gépről történő csatlakozáshoz. A szabályzat betartásával megakadályozható, hogy a Főiskola hálózatát, informatikai rendszerét a nem jogosult felhasználásból eredő károk érjék. A károk magukban foglalják az érzékeny adatok elvesztését, illetve az Főiskola belső rendszerének sérülését.

4.2. A szabályzat hatálya

A Tan Kapuja Buddhista Főiskola hálózatának távoli elérésére a Főiskolai szerver vagy routerek távoli elérésének keretében van lehetőség: intranet kapcsolat, fájlcsere szolgáltatás, távoli asztal. A szabályzat mindhárom típusú kapcsolatra vonatkozik, valamint kiegészül a szolgáltatások igénybevételénél elfogadott rendelkezésekkel.

4.3. Szabályok

A bejelentkezés időtartamára a felhasználóra érvényes A Tan Kapuja Buddhista Főiskola Hálózathasználati Szabályzata.
A rendszerbe való belépéshez szükséges a belépő személy azonosítása (felhasználói azonosító / jelszó megadása).
A belépési azonosítókat másra átruházni, illetve más azonosítóját használni nem szabad.
A belépési adatokat senkinek sem szabad elárulni.
A bejelentkezéseket ellenőrizni és naplózni kell.
Távoli bejelentkezés adminisztrátori jogokkal csak biztonságos, birtokláson és jelszón alapuló felhasználói azonosítással lehetséges.
A távoli elérésnek biztonságos kapcsolaton keresztül kell megvalósulnia (telnet helyett SSH, FTP helyett SFTP vagy SCP, vagy valamilyen biztonsági protokollon keresztül).
A bejelentkezett végpontot nem szabad felügyelet nélkül hagyni, még rövid időre sem.
5 egymás utáni sikertelen bejelentkezési kísérlet után a hozzáférést le kell tiltani.
Behívó szerveres kapcsolat esetén, ha a végpont az Internetre másik csatornán keresztül is csatlakozik, tűzfal használata kötelező.

5. Szerver biztonsági szabályzat

5.1. Bevezetés

A szabályzat célja, hogy A Tan Kapuja Buddhista Főiskola szerverére olyan követelményeket és alapbeállításokat határozzon meg, amik a biztonságos használatot elősegítik. Jelen szabályzat alapelveket határoz meg, mivel konkrét utasítások megfogalmazása a különböző szerverek különböző operációs rendszerei és szolgáltatásai miatt nehézségekbe ütközne.

5.2. A szabályzat hatálya

A szabályzat vonatkozik minden A Tan Kapuja Buddhista Főiskola tulajdonában, illetve felügyelete alatt levő szerverre.

5.3. Alapelvek

A Tan Kapuja Buddhista Főiskola hálózatába kapcsolt szervereket az rektornál be kell jelenteni, ezekről a Rektori Titkárság nyilvántartást vezet. Bejegyzetlen szerver nem működhet a Főiskola hálózatán.
A szerverekről minimálisan a következő információkat nyilván kell tartani:
A szerver fizikai helye

A felelőse (elérhetőségével együtt)
Hardver konfigurációja és operációs rendszere
Főbb funkciói és szolgáltatásai

Ezeket az információkat naprakészen kell tartani.

A szervereket a rendszergazdai szobában kell elhelyezni. A szerverekhez való hozzáférést fizikailag is korlátozni kell.

A szervereknek illetéktelen behatolástól jól védettnek kell lennie (megfelelő alapbeállítások használata, majd upgrade-k, biztonsági javítások mielőbbi telepítése).

A szerverek konzoljairól az adminisztrációs tevékenység befejeztével ki kell lépni, nem szabad felügyelet nélkül bejelentkezve hagyni.

Hacsak nem szükséges feltétlenül, nem szabad adminisztrátori jogosultságokkal használni a szervert.

A szervereken le kell tiltani minden nem használt szolgáltatást.

Ha adottak a technikai lehetőségek, a biztonságos kapcsolatfelvételt kell preferálni, adott esetben csak az ilyen típusú hozzáférést szabad engedélyezni (telnet helyett SSH, FTP helyett SFTP, SCP használata).

A szerverhez illetve szolgáltatásaihoz történő hozzáférési kísérleteket naplózni kell, és ezeket a naplókat rendszeresen ellenőrizni kell.

A biztonsági mentéseket minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni.

A biztonsági eseménynaplók, mentések esetében az őrzési idő a mindenkori hatályos jogszabályokban foglaltaknak megfelelően kell eljárni.

6. Mentési és archiválási szabályzat

6.1. Bevezetés

Az elektronikusan tárolt adatok folyamatosan ki vannak téve a hardver meghibásodásának lehetőségének, ezért a biztonság növelése és a károk csökkentése érdekében szükség van rendszeres mentésekre. Míg a mentések fő feladata a biztonsághoz kapcsolódik, addig az archiválás egy korábbi állapot tárolását szolgálja. Ez utóbbinak biztonsági incidensek bekövetkezése esetén lehet fontos szerepe, a napló és log fájlokban, valamint egyéb adatok között értékes információkat, nyomokat lehet találni a biztonsági esemény bekövetkezésével kapcsolatban. Technikai megvalósításuk hasonlósága miatt kerülnek egy helyen tárgyalásra.

6.2. A szabályzat hatálya

A szabályzat érvényes minden A Tan Kapuja Buddhista Főiskola tulajdonában, illetve felügyelete alatt levő szerverre, személyi számítógépre.

6.3. Feladatok

Ki kell jelölni azokat a személyeket, akiknek a biztonsági mentéseket illetve archiválásokat el kell végezniük. Ezt dokumentálni is kell.

Hetente teljes biztonsági mentést kell végezni a rendszerről.

A mentéseket lehetőleg úgy kell elvégezni, hogy azzal a felhasználók munkáját ne akadályozzák.

On-line rendszerek esetén hideg mentést kell alkalmazni.

A biztonsági mentéseket és archiválásokat tartalmazó adathordozókat minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni.

A mentéseket tartalmazó adathordozókon jól láthatóan fel kell tüntetni a mentett rendszer nevét, a mentés típusát és idejét.

Legalább évente visszatöltési kísérletet kell végezni a technika megfelelőségének ellenőrzése érdekében.

7. Záró rendelkezések

7.1. Felelősök kijelölése

Felhatalmazást kap a rektor, hogy a jelen szabályzatban meghatározott feladatokra az azt ellátó személyeket (felelősöket) rektori utasításban kijelölje.

7.2. Levelező listák

A Tan Kapuja Buddhista Főiskolán működő levelező listák tekintetében a lista moderátoraként megjelölt személy,

illetve szerv – a jelen szabályzatban, az Adatvédelmi és adatkezelési szabályzatban, továbbá a TKBF Szabályzataiban foglaltak figyelembe vételével – a konkrét levelezési listára érvényes „lista használati-, adatkezelési és etikai szabályzatot", jogosult meghatározni egyházi igazgatói utasítás (Buddhista tanítók, Egyház hírek, Egyháztanács, Párbeszéd, Támogatók), rektori utasítás (E-szenátus[84], Hivatalos, Tanárok), illetve – a Diákinfó esetében – Hallgatói Képviselet által elfogadott szabályozás formájában. A levelező lista adminisztrációjával kapcsolatos, a rendszergazda és a moderátor közötti feladatmegosztást a rektor határozza[85] meg, annak figyelembe vételével, hogy ki fér közvetlenül hozzá, illetve kinek áll rendelkezésére az adott feladat teljesítéséhez szükséges adat.

7.3. IT rendszer dokumentáció

A Tan Kapuja Buddhista Főiskola IT rendszer dokumentációja a jelen szabályzathoz kapcsolódó önálló dokumentum, melyet (beleértve annak későbbi módosítását is) a rektor hagy jóvá.

7.4. Szabályzat közzététele

A jelen szabályzat fő célja, hogy segítséget nyújtson az alkalmazóinak, ezért ezt a szabályzatot – a Főiskola Szabályzatainak egyéb köteteiben (HKR, FKR, EKR) szereplő adatkezelési szabályokkal együtt – közvetlenül hozzáférhetővé kell tenni az érintettek számára az erre a célra kialakítandó internetes felületen elektronikusan, valamint a Rektori Hivatalban papír alapú dokumentumként.

7.5. Hatályba lépés

Jelen szabályzat a Szenátus 2017. május 18-án kelt, 31/2017. (05.18) sz. határozata alapján 2017. május 19-én lép hatályba és A Tan Kapuja Buddhista Főiskola Szabályzatai IV. kötet: Egyéb Szabályzatok Követelményrendszere (EKR) 10. sz. mellékletét képezi. Egyidejűleg a Tan Kapuja Buddhista Főiskola Szabályzatai címlapján a IV. kötet: Egyéb Szabályzatok Követelményrendszere (EKR) kiegészül a „10. sz. melléklet: Informatikai és Biztonsági Szabályzat" megjelöléssel.

Kelt Budapesten, 2017. május 18. napján.

Jelen János
rektor

[84] Lásd: 1/2017. (07.05) sz. rektori utasítás az e-Szenatus Levelezőlista Használati-, Adatkezelési- és Etikai Szabályzatáról

[85] Lásd: 2/2017. (07.05) sz. rektori utasítás a Diákinfó Levelezőlistával kapcsolatos feladatmegosztásról.