TOMORI PÁL FŐISKOLA

INFORMATIKAI RENDSZEREK KEZELÉSI ÉS BIZTONSÁGI SZABÁLYZATA

Változat száma: 3.
Elfogadás dátuma: 2019.11.05.
Határozat száma: 2019/3/3/4.
Hatályos: 2019.11.06-tól
Felelős személy: rektor és gazdasági igazgató

A BIRTOKOS ADATAI

Név : .....

Munkakör : .....

Dátum : .....

Az elosztó aláírása : .....

Nyilvántartási szám : .....

Ellenőrzött példány: ☐ Nem ellenőrzött példány: ☐

TARTALOMJEGYZÉK

1. A dokumentum státusa és célja

A hálózat összetett, nagy anyagi és szellemi értéket képviselő rendszer. Felhasználóinak ezért vállalniuk kell a használattal járó kötöttségeket is. A hálózat nem a korlátozásokért, hanem a lehetőségekért van, és azért van szükség a korlátokra, hogy a szolgáltatások folyamatosan és biztonságosan működhessenek. Természetes, hogy a szabályzat elsősorban a biztonsági előírásokat részletezi; a lehetőségek ismertetése nem ennek a dokumentumnak a feladata.

Hálózatunk része az Internetnek, ezért szükséges, hogy szabályzatunk a nemzetközi normákhoz igazodva magában foglalja mindazokat a szigorú szabályokat és ajánlásokat, amelyek nélkül a hálózat nem működtethető, vagy működése más hálózatokra nézve veszélyes volna. Az itt leírt szabályok sokéves nemzetközi tapasztalatokon és más intézmények hasonló dokumentumain alapulnak. Betartásuk akkor is kötelező, ha valaki nem ért velük egyet vagy nincs tisztában a jelentőségükkel. Akár egyetlen ember általi megsértésük is azzal a kockázattal jár, hogy munkahelyünket kizárhatják az Internet egyes részeiből, súlyos esetben megvonhatják a főiskola Internet-hozzáférését.

Jelen szabályzás meghatározza a különböző informatikai rendszerekre vonatkozó biztonsági intézkedéseket, a szoftverek beszerzését, azok nyilvántartását és használatát, valamint az adatkezelés biztonsági szabályait, meghatározza az informatikai szerepköröket, és előírja azok feladatait.

A Szabályzat hatálya kiterjed a Főiskola összes dolgozójára, hallgatójára, és minden olyan személyre, aki a Főiskolával olyan jogviszonyba kerül, mely során az intézmény informatikai infrastruktúráját és adatvagyonát vagy annak valamely részét kezeli, vagy a Főiskola informatikai rendszerét használja.

A hálózat működéséért a jogi felelősséget a főiskola felelős vezetőjeként a Rektor viseli. A rendszergazda szakmai felelősséget vállal, hogy megteszi az Internet közössége által elvárható lépéseket a hálózat nemzetközi normáknak megfelelő biztonságos üzemeléséért.

A hálózat valamennyi felhasználója felelős az egész hálózat biztonságáért, köteles ismerni és betartani a biztonsági előírásokat és a hálózati etika alapszabályait. A felhasználók a jelszó átvételekor kötelesek jelen szabályzatot elolvasni, tartalmát magukra kötelezően elfogadni. A szabályzat nem ismerése nem mentesíti a felhasználót a megsértése esetén alkalmazható szankciók, valamint a polgári- és büntetőjogi következmények alól.

A szabályzat a szervezeti hierarchiában elfoglalt helyétől függetlenül mindenkire egyformán érvényes. A felhasználók kötelesek betartani a számítástechnikai eszközök használatát szabályozó szabályzatot. A kiemelt felhasználóknak ismerniük kell a hálózati dokumentációt, és rendelkezniük kell a szükséges szakmai ismeretekkel is.

A Főiskola alapbiztonsági fokozatba tartozik, ez a személyes adatok, üzleti titkok, pénzügyi bizalmas és nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági adatok, illetve az intézmény belső szabályozása szerinti hozzáférési jogosultság szerinti osztálya.

Az intézmény rendszerelemeiről csak a Rektor hozzájárulásával adható ki információ. Különösen tiltott az informatikai rendszerekből bármilyen információ közzététele nyilvánosan, illetve közösségi oldalakon.

A szabályzatot szükség esetén – például ha a hálózat fejlődése ezt indokolttá teszi – időről időre felülvizsgáljuk. A módosításokról a felhasználók értesítést kapnak.

2. Szoftverek beszerzése, nyilvántartása

A számítógépes programok meghatározásáért, beszerzéséért, nyilvántartásba vételéért, ellenőrzéséért és karbantartásáért a rektor által megbízott rendszergazda a felelős. A szoftverek bármilyen módosítása esetén gondoskodni kell a korábbi változat megőrzéséről mindaddig, amíg a módosítás megfelelősége be nem igazolódik.

A beszerzett programok írásos dokumentációjának egy példányát a rendszergazda őrzi.

3. A felhasználók jogai

A HÁLÓZAT TELJES JOGÚ FELHASZNÁLÓI:

- a rendelkezésükre álló lemezterület az adott személyre bízott feladatoktól függően változik, ezt használhatják az állományaik tárolására, és könyvtárukhoz (\\yume\Agora\név) bármelyik munkaállomásról hozzáférhetnek;
- elvárhatják a saját könyvtárukban tárolt anyagok bizalmas kezelését;
- használhatják a szervereken elhelyezett nyilvános programokat és más állományokat;
- használhatják a World Wide Webet és más internetes szolgáltatásokat, kivéve a pedofil, fasiszta, pornográf, vagy bármilyen módon erőszakra buzdító vagy jogellenes anyagok letöltését;
- a rendszergazda által meghatározott módon tájékoztatást kaphatnak a hálózat működésének őket érintő változásairól;
- kifejezett engedély nélkül is kihasználhatják a hálózat összes lehetőségét, feltéve, ha ezzel a jelen szabályzat előírásait, jogszabályokat, az általános erkölcsi normákat és a Netikettet, illetve más felhasználók érdekeit nem sértik.
- Egyéb, a munkával kapcsolatos file-ok kezelése (1. melléklet).

4. Az azonosító és a hálózati hozzáférés

A hálózat felhasználóinak nyilvántartása, a belépések engedélyezése és tiltása a rendszergazda első számú, elidegeníthetetlen feladata, és a hálózat biztonságos működésének alapfeltétele. A felhasználói azonosítók létrehozása és törlése ezért a rendszergazda kizárólagos joga.

Minden felhasználónak nyilvános azonosítója és titkos, csak általa ismert jelszava van. A kettő együtt teszi lehetővé a belépést. Az e-mailcím az adott felhasználó nevéből képződik: vezetéknév.keresztnév@tpfk.hu formában. Ezen címhez a felhasználó írásban kérhet tetszőleges azonosítót. Az azonosítóhoz tartozó kezdeti jelszó beavatkozás nélkül generálódik, melynek megváltoztatása az adott felhasználó feladata és felelőssége.

A hálózatba kapcsolt munkaállomások továbbra is használhatók önálló számítógépként. Ebben az esetben is szükség van azonosítóra.

Azonosítót az 1. pontban foglalt feltételek mellett a rendszergazdától lehet igényelni.

Az azonosító és a hozzá tartozó jelszó kiadására csak biztonsági alapképzés után kerülhet sor. Azonosítót kérhet – az e pontban foglaltak figyelembevételével – alanyi jogon a főiskola minden munkatársa, akit a hálózat használatától korábban nem tiltottak el, továbbá a hallgatók, akik a számukra létrehozott/engedélyezett ál-

lományokhoz férnek csak hozzá. Azonosítót csak az kaphat, aki a számítógép használatának alapjaival tisztában van. A rendszergazdának nem munkaköri feladata az alapfokú oktatás.

A főiskolai hálózatban különféle felhasználói jogokkal rendelkező csoportok hozhatók létre. A csoportok létrehozását a Rektornál kell kezdeményezni. A csoportokat a Rektor vagy az általa megbízott vezető hagyja jóvá. A csoportokhoz rendelhető jogosultságokat a Rektor az illetékes terület vezetőjével és a rendszergazdával egyezteti és meghatározza a csoporttagok körét. Ezt dokumentálni kell. A csoportok jogosultságait a rendszergazda állítja be. Ha valakinek a csoporthoz rendelt jogokon túlmenően további és/vagy eltérő jogokat kell megadni, arra a Rektor vagy az általa megbízott vezető írásban ad utasítást a rendszergazdának.

A foglalkoztatási és hallgatói viszony megszűnésével egyidejűleg a rendszergazda megszünteti az azonosítót és törli a felhasználó könyvtárát. A rendszergazda létrehozhat olyan általános, csökkentett jogokkal rendelkező azonosítókat is (pl. guest), amelyekhez nem tartozik jelszó. Az általános azonosítókkal bárki beléphet a hálózatba, akit annak használatától nem tiltottak el.

4.1. A munkatársak azonosítójának kiosztása

A munkatársak azonosítója, melyet a munkaállomásokra való belépéshez szükséges, automatikusan generálódik. Az ehhez tartozó kezdeti jelszó is automatikusan generálódik, melynek megváltoztatása a felhasználó feladata és felelőssége.

4.2. A jelszó

A jelszó mindenkinek a személyes titka, és akkor tölti be rendeltetését, ha csak egy ember ismeri. A jelszó védi a felhasználót, mert illetéktelenek számára lehetetlenné teszi az állományaiba való betekintést, leveleinek elolvasását vagy a felhasználó nevében történő jogosulatlan bejelentkezést; és védi a hálózat többi használóját is, mert lehetővé teszi a szabálysértők azonosítását. Az első jelszót a rendszergazda adja, ezt az első belépéskor meg kell változtatni. A jelszó legkevesebb hat karakterből áll. Nem lehet azonos és nem is hasonlíthat a felhasználó nevéhez, hálózati azonosítójához, telefonszámához, családtagjainak, háziállatainak, kedvenc csapatának nevéhez, születési dátumokhoz, autójának márkájához stb., és nem szerepelhet szótárban. Ajánlott jelszófajták: verssorok, dalok, mondatok kezdőbetűi, egybeírt mondatok, személyhez nem kötődő számkombinációk, különleges írásjeleket tartalmazó karaktersorozatok. Hasznosak még az Alt+számkóddal megadható speciális jelek is, azonban ezekkel éppúgy óvatosan kell bánni, mint az ékezetes betűkkel, mert a Windows alatt előállított jelszót esetleg egy DOS-os ablakban nem sikerül reprodukálni. Egyes billentyűzeteken a Z és az Y helyet cserélhet, erre érdemes odafigyelni.

A hallgatói adatbázist kezelő rendszer belépési jelszava nem egyezhet meg más célra használt jelszavakkal, különösen nem a Windows jelszóval. Szigorúan tilos a jelszót más hálózatban vagy a Windows képernyővédőjéhez, tömörítőprogramokhoz stb. használni. Fontos, hogy minden felhasználó tisztában legyen vele: vannak emberek, akik nagyon sok időt hajlandók áldozni mások jelszavának kiderítésére, hogy azzal aztán visszaélhessenek. Ehhez különböző szótárprogramokat használhatnak, amelyek a szótárban szereplő szavak kismértékű megváltoztatásával képzett jelszavakat (pl. Blöki helyett bloki, bl0ki, bloki23) könnyedén felismerik; más esetben a felhasználó személyes környezetének, szokásainak feltérképezésével jutnak olyan információkhoz, amelyek a fent említett tilalmak megszegése esetén kezükbe adják a jelszót. A betörők dolgát megkönnyíti, hogy egyes esetekben a jelszót a felhasználó a munkahelyen kívülről, Interneten keresztül is megadhatja.

A jelszót célszerű fejben tartani. Ha a felhasználó leírja a jelszót, akkor tartsa otthon, elzárva, vagy kódolja illetéktelenek számára hozzáférhetetlen módon. (Pl. ha egy vers kezdőbetűit választotta jelszónak, akkor ne a vers címét írja le, hanem valami olyan emlékeztetőt, ami csak neki juttatja eszébe azt a verset.)

A jelszót másokkal közölni, használatát másnak akár rövid időre is lehetővé tenni tilos! Ha felmerül a gyanúja, hogy a jelszót valaki megtudta, akkor azonnal meg kell változtatni, és a rendszergazdát haladéktalanul tájékoztatni kell.

A rendszergazda előírhatja, hogy bizonyos idő elteltével a jelszót kötelező legyen megváltoztatni, de ilyen előírás hiányában is érdemes ezt 1-2 havonta megtenni. Ha a felhasználó nem tartja be a jelszó kezelésére vonatkozó szabályokat, akkor a rendszergazda megváltoztathatja ugyan a jelszót, vagy rákényszerítheti a felhasználót a változtatásra, de azt elolvasni még ő sem tudja.

Általában véve a hálózati jelszót legalább olyan gondossággal kell kezelni, mint egy bankkártya PIN-kódját. A különbség, hogy a jelszó gondatlan kezelése nemcsak a tulajdonost, hanem az egész hálózatot veszélyezteti. Ha például egy megszerzett jelszóval belépve valaki betörést kísérel meg egy külső intézményben, akkor az egész főiskolát kizárhatják az internetes szolgáltatásból, a vizsgálat idejére elvihetik a hálózati szervergépeket, a tulajdonosnak pedig esetleg a rendőrség előtt kell tisztáznia magát.

A rendszergazdai jelszavakat lezárt borítékban a rektor páncélszekrényében kell elhelyezni. A boríték felbontása csak különösen fontos esetben, a Rektor és az illetékes Rektor helyettes jelenlétében bontható fel. Az esetről jegyzőkönyvet kell készíteni.

4.3. A szolgáltatások használatának szabályai

4.3.1. Mások munkájának tiszteletben tartása

A felhasználók a többi felhasználó tevékenységét szándékosan (pl. öncélú üzenetek küldése) nem zavarhatják.

4.3.2. A használat célja

A hálózat elsősorban a munka célját szolgálja. ***Az információs rendszereket minden munkatárs, felhasználó köteles a munkakörének vagy feladatának megfelelően, az adott rendszerkezelési utasításainak és kapcsolódó utasításoknak megfelelően használni.*** Tilos a politikai- vagy kereskedelmi célú használat. A felhasználóknak a hálózat használatából nem származhat anyagi haszna. Játékprogramok ***vagy egyéb más szoftverek, amelyek nem kerültek engedélyezésre a*** gépeken nem futtathatók.

4.3.3. A szoftverjog védelme

A szoftver szellemi termék, amelyben estenként sok ember több éves munkája fekszik. A főiskola tulajdonát képező programok illegális lemásolása szigorúan tilos. A gépekre csak a rendszergazdával egyeztetett szoftver telepíthető. Bizonytalan eredetű szoftver telepítése esetén kötelező a vírusmentességet ellenőrizni. Tilos a saját könyvtárakba nem jogtiszta szoftvert telepíteni, ilyent az Internetre kiajánlani, valamint az Internetről feltört programokat letölteni. Tilos crack kódokat, programindító kulcsokat e-mailben kérni, küldeni vagy felajánlani. Etikusnak tekinthető a freeware és a shareware programok letöltése, illetve a saját készítésű programok publikálása. A ti-

lalmak nemcsak a programokra, hanem minden szerzői joggal védett termékre kiterjednek, tipikusan pl. a zenei anyagokra is.

4.3.4. Ki- és belépés, a munkaállomás védelme

A hálózatba való belépéskor ügyelni kell arra, hogy a jelszót más ne lássa (normális esetben a képernyőn csak csillagokat látunk, ezért a jelszót csak akkor tudhatja meg valaki, ha rossz helyre gépeljük – pl. az azonosító helyére –, és láthatóvá válik, vagy ha a kezünkről olvassa le); továbbá arra is ügyeljünk, hogy ne adjuk meg a hálózati jelszavunkat véletlenül Windows jelszónak.

Kiemelt jogokat biztosító azonosítóval való belépés előtt a felhasználó köteles újraindítani a gépet.

A magára hagyott számítógép olyan, mintha a pólónk hátán viselnénk a jelszót. Aki leül a gép elé, elolvashatja a leveleinket, levelet írhat a nevünkben, elolvashatja és letörölheti az állományainkat, megváltoztathatja a jelszavunkat. Ez nem csak a felhasználót veszélyezteti, hanem az egész hálózat biztonságát. Ezért szigorúan tilos a munkaállomást a hálózatba való bejelentkezés után akár rövid időre is magára hagyni. Egyáltalán nem szükséges bejelentkezni, ha olyan munkát végzünk, amely nem igényli a hálózatot. A felhasználó – a guest azonosító használata kivételével – csak a gép kikapcsolása, vagy szabályos kijelentkezés után állhat fel a gép mellől. Ennek elmulasztása a belépési jog felfüggesztését eredményezheti.

A hálózatból való kijelentkezésnek biztonságos módja a gép kikapcsolása. Ha a gépet még más is használni akarja, kikapcsolás helyett a kijelentkezést is használhatjuk. (Windows alatt a logout parancs egy súlyos biztonsági hibát is tartalmaz, ezért helyette célszerű a „login guest” parancs használata. Ez kilépteti, és guest-ként újra belépteti a felhasználót, ezáltal elérhetetlenné teszi mások számára a kilépett felhasználó jogait.)

Minden felhasználó egyszerre csak egy gépről jelentkezhet be. Szabálytalan kilépés, vagy a szerver, HUB menet közbeni kikapcsolása esetén előfordulhat, hogy a felhasználó „beragad”, azaz a rendszer nem vesz tudomást a kilépéséről, és legközelebb nem engedi be. Ilyen esetben a rendszergazdához kell fordulni, az eset megelőzésére pedig be kell tartani a kikapcsolás szabályait.

4.3.5. Saját lemezterület (\\yume\Agora\név)

Az egyéni, ill. csoportjogokkal megszerzett lemezterület (kvóta) nem léphető túl. A határ túllépése esetén a lemezterület csökkenthető, ill. a felhasználó figyelmeztetése után törölhető. A lemezterület nagyságát a rendelkezésre álló erőforrások figyelembevételével a rendszergazda határozza meg. A kvóta a végzett feladatoktól is függhet.

A kvótába a levelezéshez használt alkönyvtár is beleszámít. Ezt a könyvtárat letörölni tilos! Célszerű a szabad lemezterület méretét rendszeresen ellenőrizni. Érdemes a felesleges állományokat, különös tekintettel a szövegszerkesztő biztonsági másolataira (*.bak) időnként letörölni. Fontos, hogy a levelezőprogramban a beérkező leveleket elolvasás után valamelyik folderbe (pl. Main folder) áttegyük, ugyanis az új levelek ablakában levő levelek technikai okból nagyságrendekkel több helyet foglalnak, mint a folderekben levők. Ha éppen valamelyik program használata közben fogy el a szabad hely, akkor lehet, hogy még a programból való szabályos kilépés sem lesz lehetséges, és adatvesztés történni. Ezért érdemes a szabad hely mennységét figyelemmel kísérni.

A felhasználó adataiban hardver- vagy szoftverhiba miatt keletkezett kárért a főiskola nem vállal felelősséget. Hálózaton is érvényes elv, hogy mindenről legyen biztonsági másolat.

4.3.6. A jelszavak és azonosítók védelme

A legszigorúbb tilalom alá esik, és a hálózat használatától való azonnali és végleges eltiltással jár:

- a más nevében való bejelentkezési kísérlet, akár az illető engedélyével is;
- más azonosítójának, jelszavának használata, illetve a jelszó kölcsönadása (tehát a kölcsönadásban mind a két fél vétkes!). A jelszóval elkövetett visszaélésekért a felelősség a jelszó tulajdonosát terheli;
- más jelszavának kiderítésére, állományainak, leveleinek illetéktelen elolvasására vagy módosítására tett kísérlet, a hálózat konfigurációjának megváltoztatására, a hálózaton áthaladó csomagok elfogására, a hálózati jogosultságok jelszólopó programmal, vírussal vagy bármilyen módon való megváltoztatására tett kísérlet;
- jogosulatlan belépési kísérlet külső intézmény hálózatába. Különösen barbár az ilyen cselekedet, ha külföldi gépre irányul, ennek ugyanis az lehet a következménye, hogy az szolgáltatót is letiltják a hálózatról, vagy annak egy részéről.

Megjegyzés: etikusnak tekinthető bármely külső hálózaton a guest account és az anonymous ftp kipróbálása. Nem szabad viszont bárki másnak a nevében belépéssel próbálkozni külföldön sem! Jó tudni, hogy a gépek a távoli bejelentkezéseket is naplózzák. Általános szabály, hogy amit egy hálózatban meg lehet tenni, azt nem biztos, hogy meg is kell tenni, és amit a felhasználó a hálózaton képes megtenni (pl. más felhasználókkal kapcsolatban), az nem biztos, hogy egyben etikus is!

4.3.7. A kiemelt felhasználók különös jogai és felelőssége

A rendszergazda az egész hálózat könyvtárai felett jogosultságokkal rendelkezik. Indokolt esetben más is kaphat kiemelt jogokat, ha a feladata ezt szükségessé teszi.

Annak érdekében, hogy a főiskola számítógépes rendszere védett legyen jogosulatlan használat, illetve károkozás ellen, a rendszergazdának joga van arra, hogy

- indokolt esetben bárkit a gép és a hálózat használatából kizárjon;
- megnézzen, lemásoljon, megváltoztasson vagy töröljön bármely állományt, amely kapcsolatban lehet a rendszer vagy a hálózat jogosulatlan használatával;
- a számítógépes rendszereket és a hálózatot bármikor ellenőrizze, leállítsa vagy átkonfigurálja;
- meghozzon bármely egyéb intézkedést, amely szükséges lehet a főiskola számítógépes erőforrásainak megvédéséhez, és a további működés biztosításához.

Mivel a hálózat elsősorban munkavégzési célokat szolgál, ezeknek a jogoknak egy részével a feladatok ellátása érdekében a kiemelt felhasználók is élhetnek.

A fenti jogok a rendszergazdát és a többi kiemelt felhasználót nem hatalmazzák

fel arra, hogy mások állományaiba öncélúan beleolvassanak, vagy azokban bármilyen változtatást végezzenek. Ezekhez a jogokhoz fokozott erkölcsi- és jogi felelősségvállalás tartozik. A jogosultak a tudomásukra jutott információt bizalmasan kezelik, azzal nem élhetnek vissza, a felhasználó engedélye nélkül nem hozhatják

nyilvánosságra. A titkosság alól kivételt jelent, ha az információ bűncselekmény gyanújára, vagy a hálózat működését alapjaiban veszélyeztető körülményre enged következtetni.

4.3.8. Rendellenességek jelentése

A felhasználó köteles a hálózat működésében tapasztalt rendellenességeket, a tudomására jutott jelszószerzési- és betörési kísérleteket haladéktalanul jelezni a rendszergazdának. A jelentés elmaradásából vagy indokolatlan késéséből eredő károkért az is felelőssé tehető, aki nem tett eleget ennek a kötelezettségnek.

4.3.8.1. Szoftver- és hardver hiba

A felhasználó köteles a szoftver- illetőleg hardver hibát a rendszergazdának e-mailben vagy formanyomtatványon jelezni a nyomtatvány értelemszerű kitöltésével. A nyomtatvány megtalálható a \\yume\Tpf-kozos\Szabályzatok\ISO\Nyomtatványok\Hibakezelő feljegyzés.doc hálózati helyen. Azon hardveri változtatásokat, melyek a rendszert, és annak integritását nem veszélyeztetik, a dolgozóknak is joga és felelőssége megvalósítani. A rendszergazda a rendszerért felel, az egyes munkaállomások (rendszert nem érintő) változtatását a felhasználó végzi.

Az erőforrások takarékos használata

A felhasználóktól elvárható, hogy a belső és az internetes hálózati erőforrásokkal takarékosan, másokra is tekintettel bánjanak. Ilyen erőforrások a teljesség igénye nélkül pl.: a lemezterület, a sávszélesség, a nyomtatókapacitás, a rendszergazda munkaideje. Csak olyan dolgokat töltsünk le az Internetről, amelyekre szükségünk van, és helyben nem hozzáférhetők, nagyobb anyagokat lehetőleg csúcsidőn kívül.

A hálózatban eltöltött időért a felhasználóknak nem kell közvetlenül fizetniük, de ne feledjük el, hogy – pénzzel vagy munkával – mindenért fizet valaki. Az Interneten sok ember teszi közzé munkájának eredményét ingyen, és sok szervezet bocsátja mások rendelkezésére az erőforrásait; soha ne éljünk vissza ezzel.

4.3.9. Vírusok

A felhasználóknak be kell tartaniuk a vírusok elleni védekezés általános szabályait. Ha a rendszergazda a hálózati- vagy a helyi meghajtók ellenőrzése során vírusos állományt talál, joga van azt fertőtleníteni, ha pedig a vírusirtó szoftver nem képes a fertőtlenítésre, akkor letörölni. Ilyen esetben a felhasználókat nem kell előre megkérdezni, de ha a tulajdonos személye megállapítható, akkor utólag értesíteni kell.

4.3.10. Tiltott anyagok – az internetes szolgáltatásokra vonatkozó közös szabályok

Tilos a hálózaton a jogellenes, pedofil, fasiszta, erőszakra buzdító, szeméremsértő, politikai- vagy kereskedelmi célú, ill. a szerzői jogokat sértő anyagokat tárolni, ilyeneket az Internetre kiajánlani, vagy az Internetről letölteni, a levelezőrendszert ilyen anyagok forgalmazására használni. Ilyen anyagok véletlen letöltése esetén azokat meg kell semmisíteni. A kereskedelmi oldalak kivételével tilos az ilyen weboldalakra való linkelés is. A legszigorúbban tilos a hálózatot az Internet veszélyeztetésére vagy mások munkájának hátráltatására használni. Ilyen esetben a vétkest a hálózatról azonnal és végérvényesen kitiltjuk, tettével a hatóságok előtt el kell számolnia, a munkahelynek okozott anyagi kárt meg kell térítenie.

4.3.11. Levelezés, levelezési listák

Az egyéni azonosítóval rendelkező felhasználók a rendszergazda által telepített program segítségével levelezhetnek, levelezési listákra iratkozhatnak fel. Ha a listának van belső tükrözése, akkor azt kötelező használni.

A levelezést ugyan védi a levéltitok, de technikailag a levelekhez többen hozzáférhetnek (a feladó, a címzett és a közbeeső állomások rendszergazdái), ezért biztonság szempontjából inkább levelezőlapnak érdemes tekinteni az e-mailt!

4.3.12. Adatok letöltése (www, ftp)

A rendszergazda által installált célszoftver segítségével a fenti korlátok figyelembevételével anyagok tölthetők le az Internetről. Az internetes szolgáltatások használata egyéni azonosítóhoz köthető. A meglátogatott helyeket a rendszer naplózza, így a tiltott anyagok letöltése utólag is szankcionálható. Az egyéni felhasználásra letöltött szoftverek, videók egyéb anyagok használatát a rendszergazda korlátozhatja. A főiskola hálózatán belüli „torrentezésre", torrent kliensek használatára kizárólagosan a rendszergazda adhat jogosultságot.

4.4. A Netikett

A Netikett (Netiquette) az internetes közösség hosszú idő alatt kialakított szabálygyűjteménye, melynek betartása a hálózaton való együttélés feltétele. A Netikett ismerete minden felhasználótól elvárható.

Itt a levelezésre vonatkozó legfontosabb szabályokat ismertetjük:

- Ékezeteket, HTML-kódot csak magánlevélben használj, akkor is csak ha a címzettel tisztáztad, hogy el tudja olvasni; levelezési listán, ill. a fejlécben sohasem.
- Ne használj csupa nagybetűket, mert az OLYAN, MINTHA ORDÍTANÁL. Kiemelésre használd az _aláhúzás_ jelet.
- A levél tárgya (subject) legyen informatív. Üresen hagyni illetlenség. Ne használj olyan tárgyat, hogy „Kérdés", „Segítség!", „Fontos" stb.
- Ne küldj, és ne továbbíts láncleveleket, ezeket mindenhol tiltják! Ha ilyent kapsz, töröld, és/vagy jelentsd a rendszergazdádnak. Ha olyan levelet kapsz, amelyben valamilyen e-mailben terjedő vírusra figyelmeztetnek, vagy valami veszélyre figyelmeztetnek, és kérik, hogy továbbítsd minél több embernek, ne dőlj be neki! Ezzel könnyen nevetségessé teheted magad. Az ilyen levelek gyakran ismert emberekre vagy cégekre hivatkoznak forrásként.
- Soha ne küldjél a levélhez csatolt állományokat, csak ha a címzett jelezte, hogy kéri.
- Ne kezdj veszekedést, és ne menjél bele ilyesmibe („flame"-ekbe). Az elektronikus levéllel könnyű megsérteni valakit, mert hiányzik belőle a metakommunikáció, ezért könnyen félreérthetik.

4.5. Hozzáférés a gépekhez, karbantartás

A felhasználók a hálózat hardver- és szoftverkonfigurációját nem módosíthatják. Olyan CD-ROM, amely a használat előtt telepíteni akarja magát, csak a rendszergazda engedélyével használható.

A rendszergazda, vagy az általa felkért karbantartók a karbantartás céljára vagy a hálózat normális működésének ellenőrzésére bármikor bármelyik gépet igénybe vehetik, sürgős esetben akár az ott folyó munkát megzavarva is. A hálózati szer-

verek kikapcsolásával járó munkákat a felhasználók érdekeinek szem előtt tartásával kell elvégezni, lehetőleg munkaidőn kívül. A szervereket az éppen bejelentkezett felhasználók értesítése nélkül kikapcsolni csak rendkívüli esetben szabad.

4.6. Szankciók

Annak érdekében, hogy a hálózat biztonságosan szolgálja a szabályokat betartó felhasználókat és a főiskola célkitűzéseit, a szabályzat megsértését szankcionáljuk. Enyhébb esetben, első alkalommal szóbeli figyelmeztetés is alkalmazható. Kisebb súlyú büntetéseket (pl. belépés átmeneti korlátozása, tárterület csökkentése) a rendszergazda is kiszabhat. A szokásos fegyelmi büntetéseken kívül a következő szankciók alkalmazhatók:

- lemezterület csökkentése;
- részleges eltiltás: a belépés bizonyos időre való felfüggesztése, vagy bizonyos szolgáltatások használatától való eltiltás;
- E-mail cím megvonása.

4.6.1. Saját azonosító megvonása

Különösen súlyos esetben, a szabályzat rendszeres vagy durva megsértése esetén a felhasználó ellen fegyelmi eljárás kezdeményezhető, amelynek keretében a hálózat használatától való teljes körű eltiltása is kimondható. Súlyos fegyelemsértés esetén a rendszergazda a vizsgálat idejére felfüggeszti a vétkes belépési jogát.

Lehet, hogy a fent felsorolt szabályok helyenként szigorúnak tűnnek. Reméljük azonban, hogy a rögzítésük és közzétételük az oktatási célon kívül csak a jogbiztonságot szolgálja, hiszen a felhasználók többsége soha nem is próbálkozik a megsértésükkel. A hálózat kínálta lehetőségekből sokkal több van, mint a tilalmakból, így azokat nem is lehet egy ugyanilyen terjedelmű dokumentumban összefoglalni; megismerésük hosszas tanulás eredménye lehet.

5. A munkákkal kapcsolatos állományok kezelése

5.1. Áttekintés

A mentési rendet minden esetben úgy kell megtervezni, hogy a rendszer működőképessége bármelyik komponensének kiesése vagy adatainak elvesztése esetén a legkisebb mértékű adatvesztés mellett helyreállítható legyen.

Az alkalmazások és informatikai eszközök konfigurációját annak minden módosítása után menteni kell.

A munkaállomásokon lehetőség szerint minimális mennyiségű adatot szabad tárolni.

A szerverek minden nap elmentik a munkán végzett változtatásokat, így szükség esetén vissza lehet állítani a feladat korábbi állapotait. Miután a munka befejeződött a fileokat archiválni kell.

A mentések végrajtásáért a rendszergazda felelős.

5.1.1. Napi mentések

Az adatállományok napi rendszerességgel mentésre kerülnek. Ezen mentések a szerveren erre a célra létrehozott Save(S) könyvtárba kerülnek, meghatározott fastruktúrában.

5.1.2. Dokumentumok mentése

A felhasználói szoftverek sokfélesége miatt előfordulhat, hogy a munka során keletkezett dokumentumokat egymásnak nem tudják átadni a dolgozók. Ennek a helyzetnek a megoldása érdekében minden, bármely szövegszerkesztővel készített állományt .rtf formátumban kell menteni. Az egyes dolgozók szerveren tárolt dokumentumaiért (pl.: Agora) nem a

rendszergazda a felelős, azokat legalább havi rendszerességgel az adott dolgozónak külső tárolóra kell mentenie.

5.1.3. Hivatalos levelezés

Minden céges hivatalos levelezésről egy másolat megléte szükséges, ehhez a levelező program ***másolatot kap mezőbe egy 'h' betűt kell írni***. Az így elküldött levelek egy tároló könyvtárba kerülnek, ahonnan, ezek visszakereshetőek, archiválhatóak.

A hivatalos levelezés tartalmi részét – ha lehetséges - szövegszerkesztővel íjuk meg, majd csatolt állományként küldjük el.

5.1.4. A marketing adatok felépítése és adatcseréje

Célszerű, ha az összes szolgáltatások forgalmazásában résztvevő kollega a lehető legaktuálisabb marketing adatokhoz hozzá tud férni. Ehhez ki lett dolgozva egy adat tárolási szerkezet, mely lehetővé teszi a marketingadatok egységes kezelését.

Az adott könyvtárszerkezetben elhelyezendőek a kész marketinges prezentációk, szórólapok, bemutató videók, az ezekhez felhasznált adatok (szöveg, grafika, képek, stb.).

Párhuzamosan a marketinges adatokhoz, a projektekről is vezetni kell egy rövid összefoglalót, melyeknek tartalmazniuk kell: a projekt célját, megbízót, bevetett gépeket, a grafikák és objektumok megnevezését, az elért pontosságot, időtartalmat, költségeket, valamint az esetleges továbbfejlesztéseket.

5.1.5. A saját fejlesztésű szoftveralkalmazások tárolási módja és adatcseréje

Célszerű, ha a saját fejlesztésű szoftverek gyártásában és forgalmazásában résztvevő kolléga a lehető legaktuálisabb szoftver adatokhoz hozzá tud férni. Ehhez olyan adattárolási szerkezet áll rendelkezésre, amely lehetővé teszi a saját fejlesztésű szoftveradatok egységes kezelését.

Az adott könyvtárszerkezetben elhelyezendőek az elkészült szoftveralkalmazások, a szoftverekhez készült felhasználói dokumentációk, prezentációk, szórólapok, bemutató videók, és az ezekhez felhasznált adatok (szöveg, grafika, képek, stb.).