A Katona József Műszaki, Közgazdasági Szakképző Iskola és Gimnázium számítógép-hálózatának felhasználói szabályzata (ISz)
(Röviden: Iskolai Szabályzat)

Ez a szabályzat állandóan megtalálható:
http://katonaj-bp.sulinet.hu/dokumentumok címen.

Tartalom

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 a Sulinet II.-nek és az UPC 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 iskolánkat, rosszabb esetben az egész Sulinet II. hálózatot kizárhatják az Internet egyes részeiből, súlyos esetben megvonhatják az iskola Internet-hozzáférését.

A hálózat működéséért a jogi felelősséget az iskola egyszemélyi felelős vezetőjeként az igazgató 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 - akárcsak például a közlekedésben - felelős az egész hálózat biztonságáért, köteles ismerni és betartani a biztonsági előírásokat és a hálózati etika alapszabályait. A felhasználók a jelszó átvételekor aláírásukkal igazolják, hogy ismerik és elfogadják a felhasználói szabályzatot. Ilyen aláírás hiányában dolgozó egyáltalán nem kaphat azonosítót, tanuló pedig csak akkor, ha a kötelező óraszámban

tanult számítástechnika követelményeinek teljesítéséhez ez feltétlenül szükséges; az ilyen azonosító csak korlátozott jogokat biztosít. A számítástechnika választható órakeretben történő tanulásának - ideértve az érettségire való felkészülést is - és a szakköri tagságnak feltétele lehet a szabályzat elfogadása, ha a tanmenet előírja a hálózat használatát.

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 igazgatói utasítást, az Internet használata esetén pedig a Sulinet etikai szabályzatát. (Az AUP - Acceptable Use Policy - munkacímet viselő dokumentum az interneten hozzáférhető.) A kiemelt felhasználóknak ismerniük kell a hálózati dokumentációt és rendelkezniük kell a szükséges szakmai ismeretekkel is.

A szabályzatot szükség esetén - például ha a hálózat fejlődése ezt indokolttá teszi - időről időre felülvizsgáljuk. A módosításokról a felhasználók értesítést kapnak. Ha a módosítást nem fogadják el, azonosítójukról három munkanapon belül le kell mondaniuk. Az 2004. szeptember 15. előtt kiadott azonosítók csak ennek a szabályzatnak az elfogadásával tarthatók meg.

2. A felhasználók jogai

A hálózat teljes jogú felhasználói

- a rendelkezésükre álló lemezterület mértékéig használhatják a szerverek merevlemezét állományaik tárolására, és könyvtárukhoz bármelyik munkaállomásról hozzáférhetnek;
- elvárhatják a saját könyvtárukban tárolt anyagok bizalmas kezelését;
- használhatják a szervereken elhelyezett nyilvános programokat és más állományokat;
- hivatalos vagy magánügyben szabadon levelezhetnek az iskolán belül és az Interneten keresztül;
- használhatják a Worldwide Webet és más internetes szolgáltatásokat, **kivéve a pornográf, fasiszta vagy bármilyen módon erőszakra buzdító vagy jogellenes anyagok letöltését;**
- saját honlapot készíthetnek, amelynek tartalmát tekintve olyannak kell lennie, hogy a Katona jó hírét és a jogszabályokat ne sértse;
- 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.

A hálózat az Internet felé külön BÉRELT vonalat használ, azaz nem akadályozza egyik telefonvonal működését sem; az Internet használatának költségeit az iskola és az OM fedezi.

3. 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 azonosítóból képezzük az email-címet is.
A hálózatba kapcsolt munkaállomások továbbra is használhatók önálló számítógépként. Ebben az esetben nincs szükség 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 az iskola minden tanára és nappali tagozatos diákja, akit a hálózat használatától korábban nem tiltottak el. Magántanulók és nem pedagógus dolgozók az igazgató egyedi döntése alapján juthatnak azonosítóhoz. Indokolt esetben a rendszergazda más személynek is adhat azonosítót.

Azonosítót csak az kaphat, aki a számítógép használatának alapjaival tisztában van. A rendszergazdának és a számítástechnika-tanároknak (a tanterv szerinti órákat kivéve) nem munkaköri feladatuk az alapfokú oktatás.

A (nappali tagozatos) tanulói vagy dolgozói munkaviszony megszűnésével egyidejűleg a rendszergazda megszünteti az azonosítót és törli a felhasználó könyvtárát. Ha a felhasználó másik, külső email-címmel rendelkezik, akkor kérheti az azonosító érvényességének legfeljebb fél évvel való meghosszabbítását, de ebben az időszakban a hálózatba már nem léphet be. Megtarthatják az azonosítójukat azok a dolgozók, akik a Katonából mentek nyugdíjba, ha a postafiókjukat rendszeresen ellenőrzik.

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.

3.1 A tanári azonosítók kiosztása

A tanárok és más dolgozók írásban kérhetnek azonosítót. Az azonosítót, a következő 8 karakterből állhat, ékezetes betűket, szóközöket és speciális jeleket nem tartalmazhat. Szokásos azonosítók: pl. Kovács József esetén kovacs_j.

A jelszó kiadásához szükséges biztonsági alapképzésre akkor kerülhet sor, ha elegendő jelentkező van. Azonosítót kérni elsősorban a tanév elején lehet, amikor a jelentkezők számától függetlenül mód nyílik a képzésre. Tanév közben ilyen képzés csak különleges esetben lesz. A rendszergazda fenntarthatja magának a jogot a biztonsági alapképzés megtartására és az ott átadott ismeretek számonkérésére.

Az első jelszót a belépés engedélyezésével együtt a rendszergazda adja ki. A jelszót az első belépés alkalmával kötelező megváltoztatni.

3.2 A tanulói azonosítók kiosztása

A tanulók azonosítóját a rendszergazda határozza meg. Az azonosító kiosztása osztályonként történik. Azonosítót csak azok a diákok kapnak, akik a szükséges számítástechnikai alapismereteket a tanítási órán már elsajátították. Az előírt biztonsági képzést a szaktanár tartja meg a tanítási órán, a tanmenet által előírt időben, és ő gondoskodik az ismeretek elsajátításának ellenőrzéséről. A belépést a szaktanár felelősségvállalása alapján a rendszergazda engedélyezi. Az első jelszót a szaktanár közvetítésével a rendszergazda adja ki. A jelszót az első belépés alkalmával kötelező megváltoztatni. A szaktanár köteles gondoskodni a jelszavak biztonságos őrzéséről, és csak a ténylegesen jelenlevő tanulók jelszavát adhatja ki, a hiányzók névsorát pedig az óra után haladéktalanul közli a rendszergazdával. A szaktanár és a rendszergazda közösen gondoskodnak arról, hogy belépési joga csak annak legyen, aki a képzésen ténylegesen részt vett és a jelszavát személyesen átvette. A szaktanár a hálózat használatát megtagadhatja vagy további feltételekhez kötheti, ha a tanuló a biztonságos üzemeltetéshez szükséges ismereteket nem kellő mélységben sajátította el.

A hálózat kiépítésekor első alkalommal olyan osztályok is vannak, amelyek a számítástechnikát a korábbi években tanulták. Ezeknek a képzéséről a szaktanárok egyedi módon is gondoskodhatnak.

3.3 A biztonsági alapképzés tematikája

A biztonsági alapképzés minimális tematikáját a rendszergazda határozza meg, és ez a tematika a szaktanárokat is kötelezi.

4. 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 4 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. A kis- és nagybetűk között a NetWare sem az azonosítóban, sem a jelszóban nem tesz különbséget. Egyes billentyűzeteken a Z és az Y helyet cserélhet, erre érdemes odafigyelni.

A jelszó nem egyezhet meg más célra használt jelszavakkal, különösen nem a Windows jelszóval. Ha a Windows a hálózati jelszó megadását vagy megerősítését kéri (ez rögtön a NetWare hálózatba való belépés után megtörténik!), nyomjuk meg a billentyűzeten az Esc gombot vagy kattintsunk az egérrel a Mégsem gombra. A jelszót csak a

NetWare piros fejlécű ablakában adjuk meg, vagy a Windows 95 Hálózatok ablakában, és soha ne változtassuk a Windows jelszóval együtt.

A NetWare különleges biztonsággal kezeli a jelszót, ami a Windowsról nem mondható el. Az iskolában használt beállítások mellett Windows jelszóra egyáltalán nincs szükség. 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 az iskolán 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 betartja a jelszó kezelésére vonatkozó szabályokat, akkor a rendszergazda megváltoztathatja ugyan a jelszót vagy rákényszerítheti a felhasználót a változtatásra, de 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 iskolát kizárhatják az internetes szolgáltatásból, a vizsgálat idejére elvihetik a hálózati szervergépeket, a tulajdonosnak pedig esetleg a rendőrség előtt kell tisztáznia magát.

5. A szolgáltatások használatának szabályai

Mások munkájának tiszteletben tartása

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

A használat célja

A hálózat elsősorban az oktatás és az iskolai közösségi élet céljait szolgálja, és az ilyen célú használat elsőbbséget élvez, de a lehetőségek határain belül magáncélra is

használható. Tilos a politikai vagy kereskedelmi célú használat. A felhasználónak a hálózat használatából nem származhat anyagi haszna. (A gépeken használt programok nagy részét és a hálózati szoftvert oktatási kedvezménnyel kapta az iskola, ezért a kereskedelmi használatnak az iskolára nézve jogi és anyagi következményei lehetnek.) **Videó, MP3, játékprogramok a gépeken nem futtathatók ezek figyelmeztetés nélkül törlésre kerülnek!**

A szoftverjog védelme

A szoftver szellemi termék, amelyben estenként sok ember több éves munkája fekszik. Ezért a Katona - anyagi lehetőségeihez képest - mindent elkövet a legális programok használatára. Az iskola tulajdonát képező programok illegális lemásolása szigorúan tilos. A gépekre csak a számítástechnika-tanárokkal, ill. 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 tilalmak nemcsak a programokra, hanem minden szerzői joggal védett termékre kiterjednek, tipikusan pl. a zenei anyagokra is.

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, hogy ne adjuk meg a hálózati jelszavunkat véletlenül Windows jelszónak. (A jelszót a NetWare piros fejlécű ablakában adjuk meg. Rögtön ezután felbukkanhat egy szürke ablak, amelyik a hálózatba való belépésre buzdít, és már tartalmazza a jelszót. Ilyenkor lopja el és teszi a merevlemezen mindenki számára hozzáférhetővé a jelszavunkat a Windows. Ezért itt az Esc billentyűt vagy a Mégsem gombot kell megnyomni. A hiba akkor is megtörténik, ha a bejelentkezéskor kétszer nyomjuk meg az entert.)

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 (pl. pasziánsz). A felhasználó - guest vagy a tanár 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 logout parancsot is használhatjuk. (Ehhez a Windows asztalán a Kilépés a hálózatból ikon tartozik.) Windows alatt a logout parancs egy súlyos biztonsági hibát is tartalmaz, ezért helyette célszerű a -login guest-

parancs használata. Ez kilépteti és guestként újra belépteti a felhasználót, ezáltal elérhetetlenné teszi mások számára a kilépett felhasználó jogait.

Saját lemezterület

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 fog történni. Ezért érdemes a szabad hely mennyiségét figyelemmel kísérni.

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

A jelszavak és azonosítók védelme

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

- **Ø** 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.
- **Ø** más jelszavának kiderítésére, állományainak, leveleinek illetéktelen elolvasására vagy módosítására tett kísérlet (a tanítási órán, ha ketten ülnek egy gépnél, akkor is legyenek tekintettel egymás jelszavának titkosságára)
- **Ø** a hálózat konfigurációjának megváltoztatására, a hálózaton áthaladó csomagok elfogására, a hálózati jogosultságok jelszólopó programmal, vírussal vagy bármilyen módon való megváltoztatására tett kísérlet
- **Ø** jogosulatlan belépési kísérlet külső intézmény hálózatába. (Különösen barbár az ilyen cselekedet, ha külföldi gépre irányul, ennek ugyanis az lehet a következménye, hogy az egész Sulinetet 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.

Ø a hálózat biztonsági rendszerének esetleges hibáival való visszaélés.

Aki a hálózat biztonságának hiányosságaira felhívja a rendszergazda figyelmét, ha nem követett el a szabályzatba ütköző cselekményt, jutalomban részesül.

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.

A kiemelt felhasználók különös jogai és felelőssége

A rendszergazda az egész hálózat, a számítástechnika-tanárok a saját tanítványaik könyvtára felett jogosultságokkal rendelkeznek. Indokolt esetben más is kaphat kiemelt jogokat, ha a feladata ezt szükségessé teszi.

Annak érdekében, hogy az iskola számítógépes rendszere védett legyen jogosulatlan használat, illetve károkozás ellen, a rendszergazdának joga van, hogy indokolt esetben bárkit a gép és a hálózat használatából kizárjon; megnézzen, lemásoljon, megváltoztasson vagy töröljön bármely file-t, amely kapcsolatban lehet a rendszer vagy a hálózat jogosulatlan használatával; továbbá hogy a számítógépes rendszereket és a hálózatot bármikor ellenőrizze, leállítsa vagy átkonfigurálja, illetve fenntart magának bármely egyéb intézkedési jogot, amely szükséges lehet az iskola számítógépes erőforrásainak megvédéséhez, és a további működés biztosításához. Mivel a hálózat elsősorban oktatási célokat szolgál, ezeknek a jogoknak egy részével az oktatási 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 csináljanak. 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.

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.

Az erőforrások takarékos használata

A felhasználóktól elvárható, hogy a belső és az internetes hálózati erőforrásokkal takarékosan, másokra is tekintettel bánjanak. Ilyen erőforrások pl. (a teljesség igénye nélkül): 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. Mindig legyünk rá tekintettel, hogy az internethez sok ember telefonvonalon kapcsolódik, és a kapcsolat minden másodperce pénzébe kerül, továbbá, hogy ha valakinek nagyméretű anyagot küldünk, akkor betelhet a postaládája, és esetleg más leveleit nem kapja meg. Ezért másoknak előzetes megbeszélés nélkül e-mailben csatolt anyagot küldeni vagy a másik könyvtárát szándékosan telíteni tilos!

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.

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.

Tiltott anyagok - az internetes szolgáltatásokra vonatkozó közös szabályok

Tilos a hálózaton a jogellenes, fasiszta vagy 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. Tilos az ilyen weboldalakra való linkelés is a kereskedelmi oldalak kivételével. 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, az iskolának okozott anyagi kárt meg kell térítenie.

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.

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.

Saját honlap készítése

A hálózat minden saját azonosítóval rendelkező használója készíthet személyes honlapot az Internetre. Más célú honlap készítéséhez a webmester vagy az igazgató engedélye szükséges. A honlap meg kell feleljen a jogszabályoknak, a házirendnek és a Katona által képviselt erkölcsi normáknak. A WEB-en közzétett anyagért mindenkor az oldal készítője a felelős. Az oldalon el kell helyezni az oldal készítőjének nevét, E-mail címét. A honlapkészítéshez a Netscape Composert ajánljuk, amely a tanulók és tanárok otthoni gépére is legálisan telepíthető, de bármilyen más program is felhasználható. A honlap nem esik előzetes cenzúra alá, de ha a tartalma sérti a szabályokat vagy az iskola érdekeit, akkor a számítástechnika-tanárok vagy az igazgató levetetheti, ill. kötelezheti a tulajdonost az átdolgozásra. A kész honlap belinkelését az iskola honlapjára a webmestertől lehet kérni. A honlapot a tanulói, ill. dolgozói jogviszony megszűnésekor a saját könyvtárral együtt töröljük.

6. 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. Ebben a dokumentumban nem tudjuk részletezni, megtalálható az iskola honlapjáról kiindulva a Hálózati illemtan... link alatt az RFC 1855 nevű dokumentumban. 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 küldjél és ne továbbítsál láncleveleket, ezeket mindenhol tiltják. Ha ilyent kapsz, jelentsd a rendszergazdádnak. Ha olyan levelet kapsz, amelyben valamilyen e-mailben terjedő vírusra 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 kezdjél és ne menjél bele veszekedésekbe, -flame--ekbe. Az elektronikus levéllel könnyű megsérteni valakit, mert hiányzik belőle a metakommunikáció, ezért félreérthetik.

7. Hozzáférés a gépekhez, karbantartás

A számítógépek használatát külön igazgatói utasítás szabályozza. 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 gépterem ügyeleti időben való használatának módját a számítástechnika-tanárok szabályozzák az iskola tantervében megszabott prioritások figyelembevételével. A felhasználók akkor is kötelesek betartani a felügyelő tanár utasításait, ha nem értenek azokkal egyet.

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 tanítási órát azonban a házirendnek megfelelően csak igazgatói engedéllyel zavarhatják meg. A terembeosztásban karbantartás címszóval megjelölt időben a terem csak a karbantartást végző személy engedélyével használható. A rendszergazda bizonyos munkafolyamatokat biztonsági okból csak néhány kijelölt számítógépről tud elvégezni, ezért ezekhez a gépekhez szükség esetén soron kívül hozzáférhet.

A hálózati szerverek 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.

8. Szankciók

Annak érdekében, hogy a hálózat biztonságosan szolgálja a szabályokat betartó felhasználókat és az iskola oktatási és nevelési célkitűzéseit, a szabályzat megsértését szankcionáljuk. Enyhébb esetben, első alkalommal szóbeli figyelmeztetés is alkalmazható. Kisebb súlyú büntetéseket (pl. belépés átmeneti korlátozása) a rendszergazda vagy a számítástechnika-tanár is kiszabhat. Az iskolában szokásos fegyelmi büntetéseken kívül a következő szankciók alkalmazhatók:

- Külön vizsga előírása a biztonsági tudnivalókból
- Részleges eltiltás: a belépés bizonyos időre való felfüggesztése, ill. a tanítási időre való korlátozása, vagy bizonyos szolgáltatások használatától való eltiltás.
- Email-cím, ill. saját honlap megszüntetése
- 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. Ebben az esetben a tanulónak a választott számítástechnika-óráit le kell adnia, ha a tárgyból fakultáción, szakkörön vagy érettségire előkészítő órán vesz részt, akkor azt abba kell hagynia.

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.

Budapest, 2004. szeptember 15. P.h.

Horváth Gyula
műsz.-inf. igh.

Vései Zoltán
igazgató

Tügyi László
rendszergazda