ÖK - 91 /2024

HUN REN ÖKOLÓGIAI KUTATÓKÖZPONT

Informatikai és Információbiztonsági Szabályzat és Irányelvek Felhasználóknak

Engedélyezés

Készítő	
Név:	Euline 9001:2001 Kft.
Beosztás:	irányítási tanácsadó szervezet
Dátum:	2024.03.01.

Ellenőrizte		Dokumentum jóváhagyás	
Név:	Karoliny Diána	Név:	Dr. Garamszegi László Zsolt
Beosztás:	ügyviteli osztályvezető	Beosztás:	főigazgató
Dátum:	2024.03.11.	Dátum:	2024.03. 26.

HUN-REN Ökológiai Kutatóközpont HUN REN 1.

Dokumentumtörténet

Verzió	Hatályba lépés / változás dátuma	Módosítás rövid leírása
1.0	2024.03. 26.	Első kiadás

Dokumentum adatvédelmi besorolása

Minősítés
Alap üzleti titok

1. Bevezetés

A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT a munkatársai részére folyamatosan biztosítja a munkavégzésükhöz szükséges informatikai infrastruktúrát (számítógépeket, szoftvereket, hálózatot, szolgáltatásokat, stb.), melynek üzemeltetése csak az érvényes jogszabályok, szabványok és előírások alapján lehetséges.

A számítógépes infrastruktúra (valamennyi) elemei (hardver eszközök, hálózati elemek, szoftverek) a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT tulajdonát képezik, illetve bérleti, vagy egyéb jogviszony keretében állnak a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT rendelkezésére. A szervezet tulajdonában, vagy használatában levő számítógépes infrastruktúra felhasználója köteles munkáját az alábbi szabályzat és irányelvek szerint végezni, valamint törekedni arra, hogy a tevékenységével ne veszélyeztesse a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT érdekeit és a jó hírét.

A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT fontosnak tartja, hogy nyílt és átlátható kommunikációval megfelelő szabadságot biztosítson munkatársainak a szervezet minden szintjén. Ezzel azonban együtt jár a felelősség, mely szerint minden felhasználónak védenie kell a szervezet információs és materiális tulajdonait.

2. Alkalmazási terület

A jelen szabályzat hatálya kiterjed a szervezet minden informatikai infrastruktúrát használó munkatársára, a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT-tal munkaviszonyba álló, illetve munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott munkatársakra, beleértve a szerződéses alvállalkozókat is.

3. Általános felhasználói szabályok

A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT tulajdonában, vagy használatában levő számítógépes infrastruktúra **felhasználója** KÖTELES A JELEN SZABÁLYZATBAN FOGLALTAKAT SZIGORÚAN BETARTANI.

A leendő **felhasználó** KÖTELES megismerni a jelen szabályzatot, majd ezt követően írásban köteles nyilatkozni arról, hogy a szabályzatot elolvasta, megértette és a benne foglaltakat magára nézve kötelezőnek ismeri el. Ezt a „Munkavállalói Nyilatkozat” dokumentumon köteles megtenni.

A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT a szabályzatot megszegő, illetve irányelveket nem teljesítő **felhasználókkal** szemben a hozzáférési jogosultságát az főigazgató utasítására a rendszergazda korlátozhatja, vagy megszüntetheti, súlyosabb esetben pedig FELELŐSSÉGRE VONÁST kezdeményezhet, és a szabályszegésből eredő estleges KÁROK MEGTÉRÍTÉSÉRE jogi lépéseket foganatosíthat.

4. A munkáltató jogai

A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT által üzemeltetett, illetve használt számítástechnikai eszközökön tárolt – munkavégzéssel összefüggő – információ a szervezet TULAJDONÁT KÉPEZI, így az abba történő BETEKINTÉSRŐL az **főigazgató** JOGOSULT DÖNTENI. A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT az alábbi tevékenysége során keletkezett információkat - a törvényi eseteket kivéve – harmadik félnek NEM ADHATJA ÁT.

- A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT jogosult a felhasználói IT tevékenységek folyamatos NYOMON KÖVETÉSÉRE, illetve különböző ADATGYŰJTÉSI módszerek ALKALMAZÁSÁRA:
  - lokális számítógépek merevlemezeinek TARTALMÁT MEGVIZSGÁLNI, módosítani
  - a központi gépeken (szerverek) **felhasználók** által tárolt FÁJLOKAT MEGVIZSGÁLNI
  - lokális számítógépek KÉPERNYŐJÉT MEGFIGYELNI, BILLENTYŰZETÉT ÁTVENNI
  - **felhasználók** ki- és belépését, egyes szolgáltatások igénybevételét nyomon követni, NAPLÓZNI
  - **felhasználók** elektronikus levelezését NYOMON KÖVETNI
  - **felhasználók** által látogatott Internet helyeket MONITOROZNI
  - **felhasználók** gépeire telepített programokat és azok használatát monitorozni
  - korlátozni, vagy letiltani bizonyos webhelyek elérését és/vagy bizonyos fájltípusok letöltését.

5.A munkáltató kötelezettségei

A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT **IT üzemeltetést végző rendszergazdája,** illetve az **információbiztonságért felelős személy** KÖTELES TÁJÉKOZTATNI a **felhasználókat**

- az informatikai szolgáltatásokról
- az informatikai rendszer használatával kapcsolatos valamennyi tudnivalóról
- az informatikával kapcsolatos valamennyi elérhetőségéről
- a várható üzemszünetekről, karbantartásokról
- minden egyéb újdonságról
- valamennyi, az informatikai szolgáltatásokkal kapcsolatos információról

A tájékoztatás ELEKTRONIKUS ÚTON TÖRTÉNIK, e-mail formájában.

Az **információbiztonságért felelős személy** köteles tájékoztatni a **felhasználókat** arról, hogy a rendszer milyen tevékenységeket naplóz, milyen adatállományokról készít mentést.

A nem automatizált és rutinszerű adatgyűjtési esetekben a **felhasználót** ÉRTESÍTENI KELL az adatgyűjtés tényéről.

Ha az **IT üzemeltetést végző rendszergazda** a munkavégzés során akár a helyszínen, akár távolról BELÉPNEK MÁS GÉPÉBE, arról a gép **felhasználóját** ÉRTESÍTENI KELL. Távoli belépés csak olyan módon engedélyezett, ha ez jól látszik a **felhasználó** képernyőjén is.

6.A felhasználók jogai

- A számára megítélt erőforrások biztosítását az **IT üzemeltetést végző rendszergazdától** kérni.
- A géphez hozzárendelt szolgáltatásokat a felhasználói kategóriába sorolástól függően igénybe venni.
- Az informatikai felhasználói támogatás igénybevételére.
- Meghibásodás, üzemzavar esetén az **IT üzemeltetést végző rendszergazdától** segítségét kérni.
- Hordozható gépeken (laptop, notebook) hálózatra csatlakoztatását kellő körültekintéssel a felhasználó is elvégezheti, azonban a konfigurációs beállításokon nem változtathat.

7.A felhasználók kötelességei

- A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT **által érvényben lévő, információbiztonsági előírásait tartalmazó, felhasználókra is** vonatkozó szabályokat betartani, nem rendeltetésszerű, illetve szabályzatokkal ellentétes használatot megakadályozni és jelenteni.
- A **felhasználó** a számítógépes infrastruktúrát köteles rendeltetésének megfelelően használni. a gépet tisztán tartani, a gépre vigyázni, azt csak rendeltetésének megfelelően használni.
- Az **IT üzemeltetést végző rendszergazda**, illetve az **információbiztonságért felelős személy** üzemeltetéssel, és IT működéssel kapcsolatos utasításait végrehajtani.
- A gép felhasználásával kapcsolatos fontos eseményeket, hibákat az **IT üzemeltetést végző rendszergazda** felé jelezni.
- A meghibásodás, rendellenes működés, vírusfertőzés esetén az **IT üzemeltetést végző rendszergazdát** haladéktalanul értesíteni, a gépet lezárni, s további használatát az intézkedéséig felfüggeszteni.
- Az esetlegesen felfedezett biztonsági problémákat az **információbiztonságért felelős személynek** jelenteni.
- A gépeken tárolt valamennyi információ kezelése során be kell tartani a vonatkozó ADATVÉDELMI és a SZEMÉLYISÉGI JOGHOZ fűződő jogszabályokat.
- A **felhasználónak** mindent el kell követnie a számítógépén levő, valamint az általa hozzáférhető adatok maximális biztonsága érdekében (rendeltetésszerű használat, mentések, vírusvédelem stb.)
- A **felhasználónak** mindent el kell követnie, hogy az adatok, a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT programjai, bizalmas információi harmadik fél birtokába ne juthassanak.

- A **felhasználónak** mindent el kell követnie, hogy harmadik fél programjai, adatai, információi a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT illetékességi körén belül JOGOSULATLAN FELHASZNÁLÁSRA NE kerülhessenek.
- **Átmenetileg** használaton kívül lévő munkaállomások esetében kötelező:
  - Jelszavas (X perc) képernyővédő program használata.
  - A bekapcsolt munkaállomást – ha a rajta futó alap- vagy alkalmazói szoftver ezt lehetővé teszi – manuálisan vagy automatikusan zárolt helyzetbe kell kapcsolni a munkahely (akár ideiglenes) elhagyásakor, vagy a gép használatának szüneteltetésekor.
  - Amennyiben az alkalmazói program támogatja, kötelező abban is a képernyővédő, és/vagy az automatikus kijelentkeztetési funkció használata.
- A notebookok irodán és a telephelyen kívüli szállítása, tárolása és használata során KÜLÖNÖS FIGYELEMMEL és GONDOSSÁGGAL kell eljárni az esetleges lopások megelőzése érdekében.
- A munkaállomások, perifériák fizikai védelmét elsősorban az irodák zárásával, illetéktelen személyek távoltartásával kell biztosítani. A gépek, berendezések védelméért a **felhasználó** felel.

8. Tilalmak

TILOS!

- a számítógépre szoftvert, programot telepíteni. Erre kizárólag csak az **IT üzemeltetést végző rendszergazda**, illetve az általa megbízott személyek jogosultak
- a gép konfigurációs beállításainak megváltoztatása, ideértve a különböző szintű (BIOS, illetve operációs rendszer helyi rendszergazda) jelszavak módosítása. (Különleges esetben a felhasználó indokolt kérésére az IT üzemeltető beállíthatja a gép bekapcsolásának jelszavas védelmét, azonban e jelszó későbbi megváltoztatása a felhasználó részére tilos)
- a gépek, a konfiguráció megbontása, a hardver-konfigurációs beállítások megváltoztatása, monitor vagy nyomtató cseréje, a hálózat megbontása, átstrukturálása, gépek, eszközök engedély nélküli csatlakoztatása
- más felhasználók anyagainak illetéktelen megtekintése, másolása
- **idegeneket**, nem HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT dolgozókat (**információbiztonságért felelős személy** engedélye nélkül) a saját használatú számítógéphez engedni, számukra a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT informatikai erőforrásaihoz történő bármilyen hozzáférést biztosítani
- a számítógép és a telepített szoftverek beállításainak megváltoztatása
- a meghibásodott vagy vírusfertőzött gépen tovább dolgozni, a hiba elhárítását önállóan megkísérelni

- a felhasználó számára nem engedélyezett erőforrások, szolgáltatások, jogosultságok, kvóták megszerzése. (Az erre irányuló próbálkozás, annak sikerétől függetlenül fegyelmi vétségnek minősül)
- annak megakadályozása, hogy a vírusadat fájl frissítése a gépére letöltődjön, illetve a vírusmentesítő program teljes körűen lefusson
- a víruskereső program futásának megszakítása és a víruspajzs kikapcsolása
- a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT-ban a munkavégzés során keletkezett valamennyi információt, adatot, anyagot, stb… - külön engedély nélkül-, harmadik személy részére kiszolgáltatni
- a notebookot illetéktelenek által hozzáférhető helyen, továbbá gépjármű utasterében felügyelet nélkül hagyni
- a számítógép hálózat adatforgalmát monitorozó eszközt az **IT üzemeltetést végző rendszergazda** előzetes írásbeli engedélye nélkül bárkinek használnia.
- a belső- és kapcsolódó hálózatok számítástechnikai címzési rendszerét illetéktelen harmadik fél tudomására hozni.

9. Engedélyhez kötött tevékenységek

- Számítógépek, laptopok, adathordozók irodán kívüli használata
- Különleges esetben telepítési lehetőségek engedélyezése
- Különleges esetben saját laptop használata a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT hálózatán (hálózaton kívül, illetve egyéb adathordozó csatlakoztatása nélkül megengedett)
- Ellenőrzött információ, adat harmadik személy részére történő átadása
- A **„nem”** HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT dolgozók HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT tulajdonú számítógéphez történő engedése!

10. Jelszóhasználat szabályozása

- A felhasználó a kapott jelszót az első éles belépéskor köteles megváltoztatni.
- A jelszó meghatározott idő elteltével lejár, ekkor a felhasználó csak új jelszó egyidejű megadásával léphet a rendszerbe. Ezt követően a jelszó újabb lejáratáig értelemszerűen az új jelszót kell használnia.
- A biztonság érdekében a jelszónak legalább nyolc karakterből kell állnia, és egyidejűleg legalább hármat tartalmaznia az itt felsorolt négy összetevőből (kisbetű, nagybetű, szám, írásjel). A jelszónak tehát kis- és nagybetűk, számok, esetleg írásjelek értelmetlen, illetéktelenek részéről nem kitalálható kombinációjából kell állnia.
- A felhasználó különös gondossággal köteles megválasztani jelszavait. Kerülni kell bármilyen közvetlen személyes információ jelszóként történő megadását. (Pl. családtagok, háziállat, hobbi neve) Kerülni kell nevezetes dátumok (pl. születésnap), dátum sorozatok (98jan, majd 98febr, majd 98marc stb.) megadását. Kerülni kell különböző szám-,

billentyű-, betűsorozatok, ismétlődő karakterek megadását. (Pl. ggggg, 45678, abcdef, qwertz).

- Szigorúan tilos más felhasználói nevével belépni vagy belépést megkísérelni a rendszerbe. Szigorúan tilos a más felhasználó jelszavához való hozzáférés kísérlete is. Minden ilyen irányú kísérlet fegyelmi felelősségre vonással jár.
- Tilos a jelszót másnak elmondani, megadni, vagy mások által bármilyen módon hozzáférhető helyen tárolni.
- A jelszó mások által hozzáférhetővé tételének minősül és ezért tiltott minden olyan programbeállítás, mely a felhasználói jelszó eltárolására és a későbbiek során történő automatikus megadására irányul.
- A felhasználó köteles jelszavát azonnali hatállyal megváltoztatni és az **információbiztonságért felelős személyt** értesíteni, ha arra gyanakszik, hogy jelszavát más személy megismerte, kitalálta.
- Jelszó használata tilos egyedi fájlok védelmére. Ilyen igény esetén a feladatot az **IT üzemeltetést végző rendszergazdával** együtt, megfelelő fájlhozzáférési jogosultsági rendszeren keresztül kell megoldani.
- Az **IT üzemeltetést végző rendszergazda** indokolt esetben (karbantartás, hibaelhárítás, installálás stb.) jogosultak más felhasználó nevében belépni a hálózati rendszerbe, a levelező rendszerbe, illetve más belső alkalmazásokba. Ilyen esetben – lehetőség szerint előre, ha ez nem oldható meg, akkor utólag – mindenképpen tájékoztatni kell az érintett felhasználót.
- Szigorúan tilos a jelszóhasználati biztonság bármilyen megszegése.

11. Szoftverhasználati szabályok

- A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT területén (székhelyén és telephelyein) és informatikai eszközparkján csak legális forrásból származó jogtiszta programok lehetnek. A szerzői jog által védett szoftverek illegális használata és jogosulatlan másolása törvénybe ütköző cselekedet és ennek megfelelően szigorúan tilos.
- Tilos a felhasználóknak újraformázni gépüket és nem a rendszergazda által biztosított operációs rendszert telepíteni rá.
- Tilos a szervezet tulajdonában, használatában lévő szoftverekről illegális másolatot készíteni.
- Tilos a szervezet tulajdonában, használatában lévő eszközökkel bármilyen más szoftverről illegális másolatot készíteni.
- Jogtiszta szoftver harmadik félnek történő, szerzői jogot sértő átadása szigorúan tilos.
- Általános esetben a felhasználók semmiféle szoftver installálására nem jogosultak. Ez alól az **információbiztonságért felelős személy** – különös tekintettel notebookok, illetve külső helyszíneken üzemelő gépek esetén - indokolt esetben felmentést adhat.
- Amennyiben az **információbiztonságért felelős személy** illetéktelen hozzáférést, jogosulatlan szoftverhasználatot tapasztal, azt haladéktalanul megszünteti és tájékoztatja az érintett szervezeti egység vezetőjét.

Mivel szinte napi szinten születnek új alkalmazások, rendkívül nehéz karbantartani a tiltott alkalmazások részletes és pontos listáját, de az alábbi kategóriákba tartozó összes alkalmazás tiltottnak minősül:

- A biztonsági kontrollt módosító vagy megsértő szoftverek
  - Keyloggerek – olyan alkalmazások, amelyek a Felhasználó tudta nélkül rögzítik, majd fájlba mentik vagy távoli számítógépre továbbítják a billentyűleütéseket.
  - Hálózatfigyelő szoftverek – olyan szoftverek, amelyek célja a belső hálózati forgalom naplózása.
  - Jelszófeltörő szoftverek – olyan szoftverek, amelyek célja az alkalmazásokba vagy a rendszerekbe történő behatolás a helyben tárolt jelszavak megfejtésével vagy nyers erőt alkalmazó (brute force) támadással az érvényes felhasználónév és/vagy jelszó megszerzéséhez.
  - Távfelügyeleti szoftverek – olyan szoftverek, amelyek segítségével a Felhasználók távolról bejelentkezhetnek egy PC-re, onnan fájlokat másolhatnak vagy távolról használhatják a gépet.
- Szerzői jogokat sértő szoftverek
  - Peer to peer fájlmegosztás – olyan szoftverek, amelyekkel a Felhasználók számítógépek között megoszthatnak és letölthetnek fájlokat. Tilos pl. a zenei fájlok, filmek stb. fel- illetve letöltése.

A fenti szabályok megsértőivel szemben azonnali hatállyal MUNKAJOGI INTÉZKEDÉSEKET KELL FOGANATOSÍTANI!

A jelen szabályzatban foglaltak megszegéséből eredő, a HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT kinyilvánított szándékaival ellentétes, jogosulatlan és törvénytelen szoftverhasználatból eredő valamennyi FELELŐSSÉG ÉS JOGKÖVETKEZMÉNY (ideértve a fegyelmi, súlyosabb esetben jogi, büntetőjogi eljárás kezdeményezését) az **érintett felhasználót** TERHELI.

12. Működési incidensek és információbiztonsági gyengeségek bejelentése

Bármilyen *rendellenes IT működést, rendszerleállást, kritikus rendszerhibát, egyéb incidenst* az **információbiztonságért felelős személynek**, vagy az **IT üzemeltetést végző rendszergazdának** kell elektronikus írásos formában (e-mail), vagy szóban, telefonon jelenteni.

A tapasztalt *információbiztonsági gyengeségek* bejelentése lehetőség szerint szóban történjen az **információbiztonságért felelős személy** felé.

Amennyiben a biztonsági rendszer, vagy az informatikai rendszer üzemképtelenné válik az **információbiztonságért felelős személyt** azonnal értesíteni kell.

13. Irányelvek

13.1. Az információk tartalmára vonatkozó irányelvek

Semmilyen körülmények között nem végezhető olyan tevékenység a szervezet kommunikációs rendszerein, amely sérti a törvényt vagy mások jogait. Nem tűrjük a becsületsértő, rágalmazó, zaklató szándékú vagy bárki számára fenyegető kommunikációt. Az ilyen kijelentéseket tévő **felhasználókat** jogi felelősség terheli. Példák az elfogadhatatlan tartalomra:

- Nyíltan szexuális tartalmú üzenetek, képek, karikatúrák vagy viccek;
- Trágárság, obszcenitás, rágalmazás, becsületsértés;
- Etnikai, vallásos vagy faji jellegű megbélyegzés;
- Pártpolitikai tevékenység;
- Bármely egyéb üzenet, amely úgy értelmezhető, hogy másokat nemük, fajuk, szexuális orientációjuk, koruk, nemzeti hovatartozásuk, fogyatékosságuk, vallási vagy politikai meggyőződésük miatt zaklat vagy becsmérel.

Javasoljuk, hogy a **felhasználók** közvetlenül válaszoljanak a sértő elektronikus üzenetek, telefonhívások és/vagy egyéb kommunikáció kezdeményezőjének és szólítsák fel az illetőt tevékenysége azonnali megszüntetésére. A Felhasználóknak felettesük felé is jelenteniük kell a sértő kommunikációt. A szervezet vezetősége fenntartja magának a jogot, hogy eltávolítson információs rendszereiből bármely, sértőnek vagy potenciálisan törvényellenesnek ítélet anyagot.

13.2. Internetes böngészés irányelvei

A szervezet letiltja az alább felsorolt kategóriákhoz (a videók, a grafikák, a megosztott fájlok, a böngésző plug-inek vagy a zenei fájlok) tartozó webhelyek elérését. A szervezet ezenkívül saját belátása szerint korlátozhatja, vagy letilthatja bizonyos webhelyek elérését és bizonyos hálózati szolgáltatásromlást okozó fájltípusok letöltését.

Ilyen fájltípusok lehetnek:

Lehet, hogy az irodán kívüli számítógép használatkor (pl. szállodai internet, vezeték nélküli hozzáférés kávézóban, otthoni internet) nem érvényesül a letiltás, de a **felhasználóknak** tilos szándékosan hozzáférniük a tiltott kategóriába eső webhelyekhez. Az internet dinamikus jellege miatt előfordulhat, hogy tiltott kategóriába eső webhelyek esetenként átjutnak a szűrőn. A webhelyek letiltásának hiánya ilyenkor nem jelenti azt, hogy a szervezet támogatja az ilyen oldalak megtekintését.

Nem mindenki tudja, ha képeket nézeget, filmet tölt le, folyamatosan rádiót hallgat, vagy élő közvetítést néz, akkor ezekkel a nagy adatforgalmat generáló tevékenységeket végez, és ezzel akadályozza azokat, akiknek a munkájukhoz kell sürgősen letölteni valamit az internetről.

A munkatársak az irodai internet használatában mellőzzék a következő tevékenységeket:

- Real-time videók letöltése,
- Webkamera-közvetítések,
- Játékok, filmek, zeneszámok letöltése,
- Képek nézegetése,
- On-line rádió, tv-műsor élvezete.

A szervezet által nyújtott IT-szolgáltatások, azon belül a szervezet által biztosított számítástechnikai eszközök és hálózati csatlakozás használata

esetén nem engedélyezett az alábbi tartalmi kategóriákhoz tartozó webhelyek elérése:

- Felnőtt / szexuálisan explicit
- Törvény által büntetett tevékenység
- Kémprogramok
- Szerencsejáték
- Hackelés
- Tiltott szerek
- Intolerancia és gyűlölet
- Szerzői jogvédett anyag törvényellenes megosztása
- Adathalászat és csalás
- Spamküldő URL-ek
- Erőszak
- Fegyverek
- Játékok

13.3. Elektronikus levelezés irányelvei

Az elektronikus kommunikáció nélkülözhetetlen üzleti eszköz a szervezet számára, ezért biztosítottak munkatársak részére azok az eszközök, amelyekkel lehetőségük van arra, hogy az elektronikus kommunikációba szükség szerint bekapcsolódva végezhessék munkájukat.

A szervezet elismeri, hogy a magánjellegű levelezés teljes tilalma – a publikus e-mail címek miatt is – megvalósíthatatlan, de elvárja munkatársaitól, hogy az ilyen tevékenységek minimalizálására törekedjenek, ezeket munkaidőn kívül végezzék, és rendszert elsősorban a munkavégzéssel kapcsolatos célokra használják.

- A **felhasználók** nem használhatnak a vállalat elektronikus levelezési (e-mail) címétől eltérő e-mail címet céges ügyekben (pl. nem igazolhatnak vissza szállítói rendelést egyéni e-mail postafiókból).
- Tilos az e-mail üzeneteket külső címre továbbítani.
- Hasonlóképpen tilos az indulatos levelek küldése (flaming) és a postafiókok kéretlen levelekkel bombázása.
- Az e-mail a képeslapküldéshez hasonlítható nyilvános kommunikációs eszköz, amelyen a felhasználóknak tartózkodniuk kell a hitelkártya-számok, jelszók és más kényes információk közlésétől.
- A nyílt és átlátható kommunikáció érdekében csupán kivételes esetekben (pl. az összes munkatársat érintő kommunikáció) lehet használni az e-mail titkos másolat (Blind Copy, BCC) funkcióját.

A nagyobb rugalmasság érdekében a szervezet e-mail rendszere szinte bármilyen számítógépről elérhető az interneten keresztül. Mindig válaszd a „nyilvános gép” (Public Machine) opciót, ha az e-mailt nem a szervezet tulajdonában lévő számítógépről éred el, ideértve az otthoni számítógépeket. Ez az opció korlátozza a helyi lemezre írt és onnan kijelentkezés után mások által is kinyerhető adatok mennyiségét. A nyilvános PC-től való távozás előtt mindig ellenőrizd, hogy valóban teljesen kiléptél-e a rendszerből.

A szervezet környezetének vírusfertőzésekkel szembeni védelme miatt a külső feladótól kapott vagy külső címzettnek küldött e-mail mellékleteknél

bizonyos fájltípusokat letiltunk. A leggyakoribb fájltípusokat alább felsoroljuk.

- EXE – végrehajtható állományok
- VBS – visual basic fájlok
- BAT, COM – szkriptfájlok

13.4. A szervezeti eszközök magáncélra történő használatára vonatkozó irányelvek

A szervezet eszközeinek és rendszereinek magáncélú használata engedélyezett, amennyiben csupán elhanyagolható többletköltséget eredményez, nem befolyásol negatívan semmilyen üzleti tevékenységet, nem szít ellenségeskedést a munkahelyen és nem zavarja a rendes munkahelyi feladatok elvégzését. Az eszközök a szervezet üzleti tevékenységét hivatottak szolgálni, és a felhasználók nem használhatják ezeket az eszközöket saját üzleti céljaikra (pl. saját internetes vállalkozás vitelére, vagy aukciós oldalakon történő személyes jellegű vásárlásra illetve eladásra, értékpapír-kereskedelemre).

13.5. Magánfelhasználói eszközök használatára vonatkozó irányelvek

A magánfelhasználói eszközök funkcionalitása olyan szintet ért el, amikor munkatársaink már úgy érzik, hogy használatukkal javítani tudnak a munkahelyi hatékonyságon. Jelen fejezet átmeneti irányelveket fektet le az ilyen nem standard magánfelhasználói eszközök (pl. iPhone, iPad, Android és más modern mobil platformra épülő eszközök) elfogadható használatára és a szervezet hálózatán nyújtott szolgáltatásokkal való összekapcsolásukra nézve.

A kényes adatok nem jóváhagyott külső környezetben történő tárolásának a biztonsági kockázatok mellett jogi vonatkozásai is lehetnek az esetleges külső vagy belső vizsgálatok során. Mivel a mai magánfelhasználói eszközök jelentős adattárolási kapacitással rendelkeznek, nagy információtömeg kerülhet illetéktelen kezekbe lopás, elvesztés vagy hackertámadás esetén.

Ezért a munkatársaknak felelősen kell eljárniuk, ha információt tárolnak személyes tulajdonukban lévő eszközeiken, különösen ideértve az otthoni személyi számítógépeket és a személyi mobil eszközöket. Az alábbi információkat tilos saját tulajdonú eszközökön tárolni:

- Titkos üzleti dokumentumok;
- Részletes munkatársi címtárak;
- Üzleti e-mailek és naptáradatok másolatai.

Tilos olyan szoftvert használni, amely a szervezet standard PC-s szoftverképének virtuális instanciáit futtatja (pl. a Parallels szoftver használata Apple laptopokon), mivel ilyen konfigurációknál nem lehet érvényesíteni a biztonsági patcheket és a vezeték nélküli kulcsok frissítését. Amikor a virtuális munkakörnyezet használatát konkrét üzleti okok indokolják, jóvá kell hagyatni az főigazgatóval és a szervezet tulajdonában lévő támogatott céges eszközökre kell telepíteni a megoldást, amely feladatot kizárólag a rendszergazda végezhet el.

13.6. A jogokra vonatkozó irányelvek

13.6.1 Szerzői jogok

A szavak, grafikák, videók, zenei fájlok vagy más szerzői jog által védett anyagok reprodukálásához, továbbításához, bármely formában történő újrapublikálásához, vagy terjesztéséhez meg kell szerezni a szerző illetve a tulajdonos engedélyét, és az egyéb szükséges engedélyeket.

Kifejezett ellenkező értelmű értesítés hiányában a Felhasználóknak minden interneten található anyagról feltételezniük kell, hogy szerzői jogvédelem alatt áll. Szigorúan tilos a szerzői jogvédett anyagok jogosulatlan másolása vagy felhasználása, különösen ideértve a magazinokból, könyvekből vagy más szerzői jogvédett forrásokból származó fotók és a szerzői jogvédett zenei felvételek digitalizálását és disztribúcióját, valamint az olyan szerzői jogvédett szoftverek telepítését, amelyekre nézve a szervezet nem rendelkeznek érvényes licenccel.

13.6.2 Az internetes tartalomközléssel kapcsolatos jogi felelősség

Légy tudatában annak, hogy a szervezetet is jogi felelősség terhelheti az általad írásban, vagy más módon közölt online tartalom miatt. A társaság fegyelmi eljárást kezdeményezhet a Felhasználóval szemben, ha bármilyen olyan jellegű kommentet, tartalmat, vagy képet közöl, amely becsületsértő, pornográf, magánjellegű, zaklató, rágalmazó, vagy amely ellenségeskedést szíthat a munkahelyen.

A felhasználónak tudnia kell, hogy a szervezet azon dolgozói, versenytársai, és bármilyen olyan magánszemély vagy vállalat, amely/aki becsületsértőnek, pornográfnak, magánjellegűnek, zaklatónak, rágalmazónak ítéli meg a kommentet, tartalmat vagy képet, vagy alkalmasnak tartja azt a munkahelyi ellenségeskedés szítására, az pert indíthat ellened.

Az elektronikus kommunikáció világában nem létezik magánélet. Mindig tartsd észben, hogy az internet nem anonim, és nem felejt. Az interneten leírtak valamilyen módon mindig összekapcsolhatók szerzőjükkel, mégpedig többnyire nagyon egyszerűen. Gondold végig, mi történne, ha az adott poszt széles körben ismertté válna, és hogy milyen képet festene szerzőjéről és a szervezetről.

Mindig légy tudatában annak, hogy az interneten közölt tartalom, a magánjellegű fórumban közölt tartalmat is beleértve, nyilvánosságra kerülhet és hosszú időn keresztül kereshető. A keresőprogramok a létrehozás után évekkel képesek azonosítani posztokat, a kommentek pedig továbbíthatók, vagy másolhatók. Ha valamit nem mondanál el egy konferencián, vagy egy újságírónak, akkor gondold végig, hogy helyénvaló-e azt az interneten közölnöd.

13.6.3 A közösségi médiában való részvétellel kapcsolatos jogi következmények

A közösségi média tágabb értelemben az online tartalom létrehozását és megosztását jelenti. Széles körű elterjedése megváltoztatja munkamódszereinket, ügyfelekkel, üzleti partnerekkel és egymással fenntartott kapcsolatainkat.

A felhasználóknak tudatában kell lennie, hogy a blogokban, wikikben, közösségi hálózatokban, virtuális világokban, vagy a közösségi média bármely más formájában történő részvétele jogi következményekkel járhat, és közvetlen, valós hatással lehet a szervezet hírnevére.

A Felhasználóknak ügyelniük kell a levelezőlistákra, nyilvános hírcsoportokba és bármely kapcsolódó nyilvános internetes fórumra küldött

kommentjeik és kérdéseik megfelelő strukturálására. Bármilyen anyag közlése előtt fontolóra kell venniük, hogy közlésük nem okoz-e jelentős versenyhátrányt a szervezet számára, illetve hogy az anyag nem vet-e fel PR problémákat. A Felhasználóknak azt is észben kell tartaniuk, hogy az információkat összeillesztve egy versenytárs olyan titkos információhoz juthat, amelyet aztán felhasználhat a szervezet ellen.