1. sz. melléklet

FELHASZNÁLÓK INFORMÁCIÓBIZTONSÁGI KÖTELEZETTSÉGEI

Jelen dokumentum ismerteti a legfontosabb, felhasználókra vonatkozó információkat és szabályokat, amelyek ismeretében a MÁV Zrt. (a továbbiakban: Társaság) informatikai rendszerei és eszközei eredményesen, hatékonyan, és biztonságosan használhatók.
A dokumentum az Informatikai Biztonsági Szabályzat (IBSZ) kivonatolt változata. A részletes szabályozás és a fogalmak (definíciók) leírása az IBSZ-ben, a Társaság adatvédelmi és adatbiztonsági szabályzatában és más társasági utasításokban találhatók.

Felhasználó alatt a munkavállalót vagy egyéb jogviszonyban álló természetes személyt értjük, aki informatikai eszközt és programot (alkalmazást) használ munkaköri feladatai ellátásához és ezek használatára – a szükséges szabályok elfogadását követően – hozzáférési jogosultságot kapott. A Felhasználó köteles az itt felsorolt szabályokat ismerni, munkájában alkalmazni és az informatikai biztonság fenntartásában közreműködni.

1. Bevezetés

A Társaság rohamosan növekvő mértékben alkalmaz informatikai rendszereket és infokommunikációs eszközöket az üzleti tevékenységével összefüggő nyilvántartási, adatfeldolgozási feladatokra. Jogos igény, hogy társasági adatok és adatfeldolgozó rendszerek térben és időben korlátlanul elérhetők legyenek. Ez igény kielégítése során az informatikai rendszerek és eszközök különböző biztonsági fenyegetéseknek vannak kitéve, amelyeket fel kell ismerni. Ellenük a Társaság védelmi rendszert működtet. Informatikai biztonsági szempontból elsősorban az adatok és feldolgozórendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése a fő feladat.

Bizalmasság: A bizalmasság fenntartása azt a célt szolgálja, hogy minden adat és adatszolgáltatás csak az adat megismerésére jogosultak számára legyen hozzáférhető.
Sértetlenség: A sértetlenség védelme arra irányul, hogy az adatok a feldolgozás, tárolás során csak a szándékozott és a jogosultságnak megfelelő módon és mértékben változzanak.
Rendelkezésre állás: A rendelkezésre állás biztosítása pedig azt célozza, hogy az adatok és informatikai szolgáltatások az előre megállapított körülmények között, a szükséges mértékben, az arra jogosultak számára mindig hozzáférhetőek legyenek.

Az Európai Unió kötelező érvényű jogi aktusa következtében még hangsúlyosabban jelent meg a személyes adatok védelmének igénye az elektronikus információfeldolgozó rendszerekben is, valamint előtérbe kerültek az adatkezelést végző szervezetek kötelezettségei mellett az érintettek jogai is. Kiemelten fontos, hogy az adatkezelő és az igénybe vett adatfeldolgozó által végzett adatkezelés feleljen meg a törvényi előírásoknak és a Társaság érdekeinek.

2. Biztonsági ismeretek, felelősségtudat

A felhasználó, felelősséggel tartozik az általa használt informatikai eszközök (számítógép, notebook, adattárolók, mobil- és más okos eszközök stb.), továbbá az ezeken működő programok, applikációk biztonságának megőrzéséért. Köteles továbbá a használatra vonatkozó biztonsági szabályokat (a felhasználók információbiztonsági kötelezettségeit közérthetően bemutató jelen dokumentumot, a használt rendszer üzleti tulajdonosa által elrendelt ismertetőket, felhasználói vagy üzemeltetői kézikönyveket stb.) megismerni, azokat a tevékenységnek megfelelő esetekben alkalmazni és a tőle elvárható gondossággal ellenőrizni az alkalmazott biztonsági funkciók helyes működését.

a) A felhasználó joga a Társaság által számára munkavégzés céljára biztosított eszközökkel és rendszerekkel kapcsolatosan az erre a célra fenntartott csatornákon (17. pont Elérhetőségek) bejelentést tenni, kérdést feltenni, igényt jelezni.

3. Egyéni felelősség

a) A felhasználó felelősségre vonható, ha a szolgáltatások igénybevétele során a rá vonatkozó biztonsági szabályokat tudatosan megszegi vagy nem kellő gondosságú rendszerhasználatból adódóan a Társaságnak hátránya származik.
b) A felhasználó felelős és elszámoltatható az informatikai rendszerekben végzett tevékenységéért. Az információk védelme érdekében köteles a legnagyobb gondossággal eljárni, kockázatokat mérlegelni és védelmi intézkedéseket alkalmazni vagy igényelni.
c) A munkavégzés során keletkezett adatokat a munkáltatói jogkörgyakorló a munkafeladatok ellátásával összefüggésben ellenőrizheti. További, biztonsági szempontú ellenőrzésre és az adatkezeléssel összefüggő naplóállomány bejegyzések átvizsgálására a Társaság Információ- és adatvédelem szakértői jogosultak.
d) Végfelhasználói alkalmazások (legtöbbször általános célú szoftver eszközökön alapuló megoldások, pl. Excel-táblák, makró-programok, lekérdezések, egyéni adatbázisok) nem tekinthetők informatikai alkalmazásnak. Az ezekkel előállított adatok, eredmények stb. megbízhatóságának ellenőrzése a felhasználó saját felelőssége.
e) Teszt rendszerrel és teszt adatokkal alátámasztott üzleti/vasútbiztonsági döntések nem hozhatók.
f) A felhasználó segítség igénybevétele esetén minden esetben követelje meg az üzemeltető személyzet azonosítását. Helyszíni kiszállás esetén megbízólevéllel és arcképes igazolvánnyal, illetve az üzemeltető szervezet által kibocsátott arcképes munkavállalói igazolvánnyal, távkarbantartás esetén – amennyiben nem Ön kérte a segítséget – a HelpDesk-en keresztül igazoltassa a távoli karbantartó bejelentkezésének jogosságát.
g) A felhasználó kísérje figyelemmel az általa használt számítógépes munkaállomást érintő üzemeltetési, (táv)karbantartási tevékenységet, legyen jelen ezek végzése során.
h) A felhasználónak bejelentési és együttműködési kötelezettsége van, amennyiben felmerül annak a gyanúja, vagy olyan eseményt észlel, amely hibára vagy a biztonsági szabályok megsértésére utal. Ebben az esetben a problémát a lehető legrövidebb időn belül jelenteni köteles a HelpDesk részére.
i) A felhasználó a jelszava által aktivált eszközt rövid időre sem hagyhatja felügyelet nélkül. Ideiglenes távollét esetén köteles működtetni az informatikai eszköz jelszavas védelemmel ellátott képernyővédő funkcióját (a Windows+L billentyű egyidejű lenyomásával), ha munkahelyét – akár rövid időre is – elhagyja, vagy egyéb módon gondoskodjon a számítógép mások általi használatának megakadályozásáról (pl. a kizárólagosan használt helyiség bezárása).
j) A felhasználónak figyelmet és megfontoltságot kell tanúsítania az általa birtokolt vagy kezelt adatok mással történő megosztása esetén az információ- és adatvédelemmel

kapcsolatos szabályok betartására, a megosztás során igénybe vett hálózati szolgáltatás biztonsági követelményeinek alkalmazására.

4. Felhasználói jogosultság

a) A felhasználó a részére meghatározott munka elvégzéséhez szükséges mértékű hozzáférést kap az informatikai rendszerekhez „a szükséges minimális jogosultság” elvének alapján, az adott rendszerre vonatkozó felhasználó-adminisztrációs eljárásoknak megfelelően.
b) A felhasználó köteles a vezetője által engedélyezett (jogosultsági) határokon belül dolgozni és nem tehet kísérletet azon rendszerek, alkalmazások, funkciók, adatok elérésére, amelyekre nincs feljogosítva.
c) A felhasználó kizárólag technológiailag indokolt esetben, az adott munkafeladat végrehajtásának idejére, illetve időszakára kérhet, és– határozott időre, de legfeljebb 1 évre kaphat rendszergazdai jogosultságot. Az időtartam leteltét követően az igényt újra be kell nyújtani, amelynek hiányában a jogosultságot vissza kell vonni.
d) A felhasználó a vonatkozó engedélyező és adminisztrációs eljárások után hozzáférést kaphat az IBSZ-ben ismertetett hálózati szolgáltatásaihoz.

5. Jelszavak használata

A felhasználónak a jelszava védelme érdekében a következő szabályokat kell betartania:

a) Tudatában kell lennie, hogy mindazon műveleteket, melyeket az ő azonosítójával és jelszavával bárki végrehajt, az informatikai rendszer az ő „terhére” könyveli el. Ezért a jelszavát kellő körültekintéssel kell kezelnie, azokat más személyeknek nem adhatja meg, nyilvánosságra nem hozhatja, köteles azok titkosságát megőrizni. A felsoroltakért személyesen felelős.
b) Más nevében (a delegálás esetét kivéve) nem tevékenykedhet.
c) Még delegálás esetén sem léphet be más nevében a rendszerbe, és nem kezdeményezheti más bejelentkezési jelszavainak megismerését.
d) A jelszó házirend betartása minden felhasználóra kötelező. A jelszó hossza, bonyolultsága, a cserélésének periódusa stb. a kötelező alapbeállításokhoz képest szigorúbb irányban rendszerenként eltérhet. Alapszabály, hogy a jelszó nem egyezhet meg a felhasználói azonosítóval és a jelszó csere során az előző jelszóval.
e) A jelszó kívülálló számára ne legyen egyszerűen kitalálható, ne egyezzen meg a szótárakban előforduló szavakkal, ne tartalmazzon a felhasználóra, vagy hozzá közel álló személyekre, tárgyakra stb. utaló információkat (pl. neveket, telefonszámokat, születési dátumokat, gépjármű forgalmi rendszámát, kedvenc háziállata nevét), és összefüggő szövegként ne legyen olvasható.
f) A felhasználónak el kell kerülnie a Társaság rendszerében hálózati bejelentkezésére használt jelszóval megegyező jelszó megadását az általa használt informatikai rendszerekben.
g) A jelszavakat nem szabad felírni, papíron tárolni. Amennyiben ez elkerülhetetlen (pl. nem megváltoztatható rendszergazdai és egyéb technikai jelszavak), akkor gondoskodni kell a jelszó zárt borítékban, a közvetlen vezetőnél történő, biztonságos tárolásáról.
h) Amennyiben a felhasználó megtudja, vagy azt gyanítja, hogy jelszavát valaki megismerte, azonnal le kell azt cserélnie és a felmerülő biztonsági kockázat lehetőségéről tájékoztatni kell az információ- és adatvédelemért felelős vezetőt.

i) Amennyiben a hitelesítési folyamatban a beírt jelszó a képernyőről vagy a billentyűzetről begépelés során leolvashatóan más számára is megismerhető, a felhasználó köteles oly módon eljárni, hogy a jelszót illetéktelen személy ne láthassa meg.
j) A felhasználó a részére generált első jelszót, a legelső bejelentkezése alkalmával köteles módosítani.

6. Társaság eszközeinek használata

a) A felhasználók – eltérő írásbeli megállapodás hiányában – nem jogosultak a Társaság infokommunikációs erőforrásai (a nem nyílt informatikai alkalmazások [szoftvertermékek, szolgáltatások], az infokommunikációs eszközök [munkaállomás, laptop, okostelefon, perifériák stb.], a belső hálózat, az internet, továbbá az adathordozók [mágneslemez, CD/DVD stb.]) személyes célú használatára.
b) Az infokommunikációs erőforrásokhoz való hozzáférés és azok használata kizárólag megfelelően azonosított, hitelesített és jogosított felhasználók számára engedélyezett.
c) A Társaság külön engedélye nélkül tiltott a felhasználó számára az, hogy nem a Társaság által biztosított eszközzel vegye igénybe a Társaság nem nyilvános informatikai szolgáltatásait. Ezeken a Társaság adatait nem tárolhatja.
d) A Társaságnál csak a hivatalos csatornákon keresztül beszerzett, elfogadott és installált hardver (pl. szkenner, digitális fényképezőgép) és szoftver, illetve adathordozó (pl. CD/DVD, pen-drive, külső HDD stb.) használható.
e) Társaságon kívüli adathordozó (pl. külső fél bemutatója) csak abban az esetben használható Társasági informatikai eszközön, ha az nincs a hálózatra kötve és az eszközön frissített az operációs rendszer és működik a szintén folyamatosan frissített kártékony kód elleni védelem (víruskereső szoftver).
f) Olyan szoftvert, amely valamilyen módon kikerüli a jóváhagyott védelmi eljárásokat vagy ellenőrzéseket, tilos az informatikai eszközökre telepíteni, az interneten keresztül használatba venni.
g) A munkaviszony megszűnése, a munkakör megváltozása, vagy más, a munkahelyi vezetője által támasztott igény esetén a felhasználónak minden eszközt és információs erőforrást, vissza kell szolgáltatnia. Ekkor az általa használt informatikai eszközön és rendszeren tárolt személyes adatait törölnie kell vagy erre vonatkozó felhatalmazó nyilatkozatot kell kiadnia. Ennek birtokában az üzemeltető személyzet végzi el a törlést. A számítógépén, általa használt rendszerben csak a munkafeladatok további elvégzéséhez szükséges adatállományok maradhatnak.
h) A Társaság számára végzett hivatalos külföldi munkavégzés céljára saját tulajdonú eszköz a nem alkalmazható. Külföldi tartózkodás esetén a Felhasználó köteles betartani a Társaság által előírt, eszköz- és rendszerhasználatra vonatkozó járulékos biztonsági követelményeket.
i) A Társaság által munkavégzésre biztosított mobil(okos)telefonok esetében a feltöltött alkalmazások potenciális veszélyforrást jelentenek a készülék adataira, ezért a felhasználónak kellő óvatosságot és figyelmet kell tanúsítania azok kiválasztásánál.
Mobiltelefon használati szabályok:
   - tilos ellenőrizetlen forrásból, a HelpDesk útján kiadott IKI engedély nélkül alkalmazást feltölteni,
   - a rendszer- és alkalmazásfrissítések futtatását engedélyezni kell,
   - a telefon képernyőjét – használaton kívül – képernyővédővel kell zárolni vagy automatikusan zároltatni az illetéktelen hozzáférés megakadályozása érdekében, amely legalább PIN kóddal, még inkább jelszóval, illetve biometrikus azonosítással oldható fel,

- tilos a Társaság által beállított eszközparamétereket, beállításokat megváltoztatni.

7. Védendő információk megőrzése

a) A felhasználó senki előtt nem fedheti fel a Társaság védendő információját, kivéve, ha arra jogosult azt engedélyezi. Ebbe beletartoznak a Társaságra, valamint ügyfeleire, informatikai rendszerére és szoftverfejlesztésére, termékeire és szoftverlicenceire vonatkozó védendő technikai információk is.
b) Kerülni kell a Társaság védett informatikai környezetből a védendő információ kimásolását, indokolatlan továbbítását.
c) Védendő információnak a Társaság védett informatikai környezetéből való kijuttatása csak az erre vonatkozó, kifejezetten megengedő szabályok szerint és módon történhet.
d) Védendő információt titkosított módon másolható hordozható adattárolóra, vagy – amennyiben rendelkezésre áll – az adathordozó titkosító mechanizmusát kell alkalmazni.
e) A védendő, elektronikus formában megjelenő információt tartalmazó hordozható eszközt használaton kívül az IBSZ előírásai szerint kell elzárni.
f) Az informatikai biztonsági intézkedéseket és a Társaság egyes rendszereire vonatkozó belső szabályait oly módon kell kezelni, amely megakadályozza azt, hogy illetéktelen személy számára hozzáférhetővé váljon.
g) A felhasználó által használt adattárolásra alkalmas eszközöket és adathordozókat (pl. számítógép, mobil telefon, merevlemez, CD/DVD) az adatokat újrafelhasználás vagy selejtezés előtt a szokásos eszközökkel, helyreállíthatatlan módon – az üzemeltető szervezettel – le kell töröltetni. A védendő információt tartalmazó adathordozót selejtezés előtt adatmentesíteni kell az adat helyreállíthatatlan felismerhetetlenné tételével vagy az adatot tartalmazó adathordozó teljes fizikai megsemmisítésével.
h) A védendő információt tartalmazó kinyomtatott papírokat az iratkezelési szabályok szerint kell kezelni.
i) Az adatszivárgás megelőzése érdekében – műszaki lehetőségek megléte esetén – technikai megvalósítással is elősegíti a Társaság a felhasználót abban, hogy megakadályozza, korlátozza, illetve jelezze a védendő adatok kijutását az informatikai hálózatból.

8. Adatok biztonsági mentése

a) A felhasználónak – az adatbiztonság megőrzése érdekében – a Társaság által biztosított központi tárhelyet (pl. Sharepoint, fájlszerver) kell igénybe vennie a védendő információk tárolására. Nem maradhat el a letárolt adatokat rendszeresen felülvizsgálata, a már nem szükséges vagy jogszerűen már nem feldolgozható információkat a felhasználónak törölnie kell.
b) Az informatikai rendszerek rendelkezésre állását minden felhasználónak elő kell segítenie, ehhez HelpDesk segítséget kérhet az általa használt adatok rendelkezésre állásának biztosítása érdekében (pl. rendszeres mentés hálózati szerver tárhelyre, SharePoint tárhelyre).
c) Az informatikai rendszer működésképtelensége esetén minden felhasználó felelősséggel tartozik a szolgáltatások helyreállításának támogatásáért.
d) Az engedéllyel különféle titkosított hordozható adattárolókon tárolt adatok kizárólag másolatok lehetnek, az eredeti adatoknak mindig központi tárhelyen, vagy a munkaállomáson kell rendelkezésre állniuk.

9. Kártékony kódok elleni védelem

a) Az installált kártékony kód elleni védelmet (vírusvédelmet), illetve azok frissítését tilos hatástalanítani. A védelemmel kapcsolatos eseti utasításokat pontosan és haladéktalanul végre kell hajtani.
b) Vírusfertőzést vagy annak gyanúját (pl. a munkaállomás szokatlan, megbízhatatlan viselkedése, lelassulása, érthetetlen vagy nem indokolt rendszerüzenet megjelenése) haladéktalanul jelenteni kell a HelpDesk-nek.

10. Szoftver tulajdonjog

a) A felhasználók:
   - a munkaköri leírásban előírt feladatukon túlmenően nem installálhatnak, nem fejleszthetnek, nem karbantarthatnak, vagy nem tölthetnek le szoftvert (beleértve az ún. szabad-felhasználású, freeware, shareware stb. programokat is) a Társaság munkaállomásaira,
   - a Társaság munkaállomására installált szoftvert nem másolhatják le más helyen történő használat céljából,
   - ha kétség merül fel a szoftver szerzői jogai felől, akkor kapcsolatba kell lépni az ITRF szoftver licenc-nyilvántartásáért és installációjáért felelős munkatársával.
b) A szerzői jogok megsértése törvénybe ütköző cselekmény, ezért felelősségre vonáshoz vezethet, akár a felhasználó elleni büntetőeljárás megindítását eredményezheti.

11. Informatikai eszközök fizikai védelme

a) A felhasználóknak szállítás közben a lehetőségei határain belül személyesen kell vigyázniuk a hordozható informatikai eszközeikre (pl.: notebook, okostelefon).
b) A hordozható eszközöket irodán kívül zárható íróasztalban vagy szekrényben kell tartani, fizikailag el kell zárni vagy – amennyiben technikailag lehetséges – különleges (pl. Kensington) zárat kell alkalmazni az eszköz biztosítására.
c) Meg kell óvniuk a hordozható adattároló eszközök (CD/DVD-k, pendrive, HDD-k stb.) fizikai állapotát.
d) Az eszközöket védeni kell a nem kívánatos fizikai és környezeti hatásokkal szemben. (túlzottan magas vagy alacsony hőmérséklet, folyadék stb.)
e) Az informatikai eszközök külföldre történő kivitelére és külföldi használatára vonatkozó külön szabályokat a kiutazás előtt meg kell ismerni.
f) A felhasználók kötelesek távol tartani az informatikai eszközeiktől, valamint a kinyomtatott dokumentumaiktól a hozzáférési jogosultsággal nem rendelkező személyeket. Közvetlen munkakörnyezetükben kötelesek kérdőre vonni a kíséret nélkül megjelenő idegeneket.

12. Távoli hozzáférés

A felügyeleti vagy rendszeradminisztrációs céllal távoli hozzáféréssel rendelkezőkre külön szabályok vonatkoznak.

A felhasználó részére a távoli hozzáférést a munkáltatói jogkörgyakorló vezető engedélyezheti. Távoli hozzáférés során a felhasználó (jellemzően VPN-en keresztül) úgy éri el a megszokott munkakörnyezetét valamely külső helyről (pl. otthonról), mint ha ezt az irodájából tenné, ezért az alábbiak betartása szükséges:

a) Ha a Társaság távoli hozzáférésre engedélyt ad, fenntartja magának a jogot, hogy rendszeresen megvizsgálja a kapcsolattal összefüggésben keletkezett napló állományokat, a hívások adatait, és szúrópróba szerinti ellenőrzést végezzen annak meghatározására, hogy a gyakorlati kivitelezés megfelel-e a vonatkozó előírásoknak.
b) Távoli hozzáférésre a Társaság által biztosított eszközöket szabad használni, ettől külön engedély birtokában lehet eltérni. Nem a Társaság tulajdonába tartozó eszközzel megnyitott távoli hozzáférés során biztosítani kell az eszközhöz illetéktelen hozzáférés megakadályozását (pl. jelszavas képernyőzár) olyan személyek részéről is (pl. családtagok), akik az adott eszközt egyéb célból jogszerűen használhatják.
c) Az informatikai eszközön a társasági és rendszerszintű IBSZ által meghatározott kártékony kód elleni védelemnek (vírusvédelemnek), a biztonsági frissítéseknek (javítócsomagok, patch-ek) és biztonsági eszközöknek telepítve kell lenniük, ezeket kötelező folyamatosan használni és frissíteni, azokat eltávolítani tilos.
d) Kiemelt biztonsági osztályú rendszerhez távolról hozzáférni többtényezős hitelesítéssel megengedett.
e) A távoli hozzáférésre használt gépen védendő információt tárolni csak, megfelelő kódolási eljárást alkalmazva szabad. A felhasználónak gondoskodnia kell ezen információk rendszeres mentéséről és a mentések megfelelő védelméről (pl. lopás vagy adatvesztés ellen).

13. Internet-használat

a) Az internetre történő csatlakozás a Társaság belső hálózatára csatlakozott eszköz esetében a kialakított tűzfalas védelmi rendszeren keresztül engedélyezett.
b) A Társaság hozzáférési pontjairól a felhasználó részére az internetre kapcsolódás lehetőségének kialakítását és az internetes szolgáltatások használatát valós üzleti céloknak kell indokolniuk, és azt a közvetlen vezetőnek kell jóváhagynia.
c) Az internetről csak olyan állományok tölthetők le, amelyek a munkavégzéshez feltétlenül szükségesek.
d) A Társaság az internetes tevékenységet monitorozza, kontrollja alatt tartja. Ennek keretében a titkosított adatcsomagokat is a határvédelmi rendszerekkel (IPS, DLP stb.) kibontva megvizsgálhatja. A Társaság az internet hozzáférés biztosításának és használatának szabályairól szóló utasításban meghatározottak szerint korlátozza az adatforgalmat.
e) A potenciális rosszindulatú kódokat tartalmazó weboldalak és szolgáltatások szűrésére a Társaság megfelelő eljárást alkalmaz. E körbe tartoznak többek között a fórumok, blogok, chat-oldalak, file- és videó-megosztók, közösségi portálok, a jó ízlést sértő, pornográfiát vagy szélsőséges, illetve indokolatlan erőszakot tartalmazó oldalak, továbbá on-line játékok, TV-k és rádiók. Kizárólag a munkával közvetlen összefüggésben engedélyezhető ezek használata.

14. Elektronikus levelezés

Az elektronikus üzenetváltás (e-mail) a Társaság hivatalos kommunikációja, amely szolgáltatás az üzleti információcsere sebességének fokozásával a munka hatékonyságának növekedését segíti elő.

A felhasználó köteles betartani a vonatkozó eljárási, üzemeltetési és etikai utasításokat, irányelveket, beleértve, de nem kizárólag, az alábbiakat:

a) Mivel a levelező rendszer kizárólag a Társaság feladatainak végrehajtására szolgál, a felhasználónak tájékozottnak kell lennie arról, hogy a Társaság levelező rendszerén tárolt és továbbított levelek a Társaság tulajdonát képezik, ezért a Társaság szabályzataiban feljogosított ellenőrző szervezeteknek ezekhez az állományokhoz a vizsgálathoz szükséges mértékig betekintési joguk van. A személyes adatokat érintő betekintés szabályait a Társaság Adatvédelmi és adatbiztonsági szabályzata tartalmazza.
b) A felhasználó elektronikus leveleinek archiválása és karbantartása (az időszerűtlen és szükségtelen üzenetek törlése) a postafiók tulajdonosának feladata és felelőssége.
c) A postafiók tulajdonosa még helyettesítés okán (pl. szabadságra távozás miatt) sem adhatja át más személy(ek) részére levelezőrendszerbeli azonosítóját és jelszavát. Indokolt esetben ideiglenes olvasási jogot adhat másoknak a saját email fiókjához a megfelelő eljárás szerint, de ezt az indok megszűnésekor azonnal vissza kell vonnia.
d) A Társaságtól való távozás vagy áthelyezés esetén – a munkakör átadási folyamat részeként, indokolt esetben – rendelkezni kell automatikus e-mail üzenet kiküldéséről, amely azt tartalmazza, hogy a postaláda tulajdonosa már nem tölti be a beosztást, valamint megjeleníthető az adott feladatot a továbbiakban ellátó felhasználó elérhetősége.
e) A felhasználók – a munkavégzéssel való összefüggés esetét kivéve – nem adhatják ki munkatársaik e-mail címét, különösen nem a teljes címlistát.
f) A Társaság levelezőrendszere – az arra feljogosított felhasználók számára – az interneten keresztül bárhonnan elérhető, amely használata során be kell tartani az alkalmazott hozzáférési módnak (Outlook Web Access, ActiveSync vagy Outlook Anywhere) megfelelő, speciális biztonsági szabályokat.
g) Magáncélra kialakított (pl., Gmail, Freemail, Citromail stb.) postafiók használata a Társaság hálózatába kapcsolt munkaállomásról nem megengedett.
h) Tilos a Társaság levelezőrendszeréből a beérkező üzenetek automatikus továbbítása bármilyen külső e-mail cím(ek)re. Az átirányítást a Társaság technikai eszközökkel korlátozhatja. Szabadság, hosszabb távollét esetére beállítható automatikus válaszban (ha szükséges) helyettest kell megjelölni. A válasz alapján a küldő felelőssége eldönteni, hogy a helyettesnek megküldi-e a kérdéses üzenetet.
i) Az elektronikus levelező rendszer nem használható fel a Társaság üzletmenetéhez nem kapcsolódó célokra.
j) Védendő információnak minősülő adatokat kizárólag a külön szabályzatban engedélyezett módon szabad tárolni, illetve továbbítani.
k) Társaságon kívüli címre küldendő levél mérete ne haladja meg a 10 Mbyte méretet, kivéve ha előre egyeztetetten arra alkalmas a fogadó levelező rendszer.
l) A levelező rendszerben egyidejűleg maximálisan 100 címzett számára engedélyezett üzenet küldése, amely alól az információ- és adatvédelemért felelős vezető adhat felmentést. A levelező rendszerben a 100 címzettet meghaladó csoportcímekre történő küldést jogosultsághoz kell kötni. Ezekre a címekre a küldő jogosultságot a BIF IAV vezető engedélyezi.
m) Tilos lánc- vagy kéretlen elektronikus leveleket másoknak küldeni, továbbítani, azokra válaszolni. A csatolt anyagokban könnyen terjedhetnek rosszindulatú kódok is, valamint könnyen összeállítható belőle a levélelőzmények (címzettek) alapján egy e-mail cím lista amely szintén veszélyeket hordoz magában. Aki ilyet kap, az köteles az üzenetet – lehetőleg elolvasás, és továbbküldés nélkül – törölni, illetve HelpDesk-et értesíteni. A Társaság fenntartja magának a jogot az ilyen üzenetek kézbesítésének megakadályozására.
n) A küldőnek ellenőriznie kell, hogy a cím, amelyre üzenetet küld korrekt, és az illető személy jogosult az információ kézhez vételére.
o) A levelek továbbküldése vagy válaszadás során minden esetben egyedileg kell mérlegelni a címzettek körét és a benne foglalt, vagy a mellékletként csatolt információk tartalmát,

annak érdekében, hogy azok illetéktelen felhasználók kezébe indokolatlanul ne kerüljenek.

p) E-mail küldése során ne csomagoljunk információt QR kódba.
q) Beérkező rasszista, gyalázkódó vagy gazdasági bűncselekmény gyanúját keltő üzenetről a HelpDesk-et azonnal értesíteni kell.
r) Ismeretlen helyről vagy személytől származó levelek érkezése estén, fokozott elővigyázatosságot kell tanúsítani. Amennyiben feltételezhető, hogy kéretlen levélről van szó, abban az esetben tilos azt megnyitni. Ha a levél megnyitását követően észlelhető a levél kéretlen jellege, tilos a hivatkozásokat, illetve a hozzá csatolt mellékleteit megnyitni vagy elmenteni. Ezeket a leveleket a felhasználó köteles olvasatlanul, azonnal törölni.

Az elektronikus levelezés során továbbított, fogadott információk bizalmassága és sértetlensége a küldő és fogadó rendszerek együttes biztonsági beállításainak függvénye. Épp ezért a Társaság szempontjából nagy anyagi vagy reputációs kockázatot jelentő küldemények bizalmasságának és sértetlenségének növelése érdekében a küldeményt – a küldő/fogadó partnerrel eltérő kommunikációs csatornán egyeztetve – célszerű fokozott védelemmel (pl. küldemény titkosítása, küldemény visszaigazolása) ellátni, amihez a HelpDesk segítsége igényelhető.

15. Adathalászat elleni védelem

Az adathalászat olyan csaló szándékú tevékenység, amelynek fő célja a címzett anyagi megkárosítása. A felhasználó tájékozatlanságát, hiszékenységet kihasználva ráveszik, hogy megadja személyes adatait vagy megtévesztéssel kártevő kód futtatására késztetik.

a) A felhasználó köteles kellő megfontoltságot tanúsítani a levelező rendszer illetve az internet használat során. Gyanú esetén ne nyissa meg a csatolmányt és semmiképp ne adja meg a személyes adatait. Fokozott figyelmet és óvatosságot tanúsítson, ha a beérkező üzenet:
    - jutalmat vagy könnyű nyereményt ígér,
    - helyesírási hibákkal teli, megnyitásra vagy klikkelésre ösztönöz,
    - ismeretlen feladótól érkező, vagy ismert feladótól érkezett de nem várt üzenet esetén a tartalomtól függően más csatornán vegye fel a kapcsolatot a feladóval és győződjön meg a küldemény hitelességéről.

b) Hivatkozást (linket) tartalmazó üzenet esetén:
    - Ellenőrizze a hivatkozás helyességét. Vigye az egeret a hivatkozás fölé, de ne kattintson rá, és nézze meg, hogy a cím megegyezik-e az üzenetben megadott hivatkozással.
    - Győződjön meg arról, hogy a hivatkozás nem tartalmaz véletlen (esetleg szándékos) elírást, amely az adott intézmény/szervezet web oldala helyett esetleg hamisított oldalra vinné (pl. www.microsoft.com helyett a www.mircosoft.com).
    - Utasítsa vissza, ha egy rendszerüzenetben programkód végrehajtásra vonatkozó engedélyét kérik.

További gyanú, esetleg bebizonyosodott adathalászati kísérlet esetén haladéktalanul vegye fel a kapcsolatot a HelpDesk-el!

16. Az információbiztonsági események és gyenge pontok jelentése

a) A felhasználó a felmerült biztonsági problémáról köteles haladéktalanul jelentést tenni az informatikai működéstámogató személyzetnek kell jelenteni (HelpDesk). Az esemény kivizsgálása során a felhasználónak a kivizsgálást végzőkkel együttműködési kötelezettsége van.
b) A felhasználó ne kezdjen hozzá az események, hibák önálló kezeléséhez vagy feltárásához, mert ez a szabályzatban meghatározott szervezetek feladata.

Teendők rendszer-, illetve alkalmazáshiba esetén:

- A hibaüzeneteket képernyőmentéssel kell megőrizni, és a HelpDesk részére mielőbb továbbítani.
- Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás vagy kártevő kód (pl. vírus) okozta, gondoskodni kell az érintett munkaállomás hálózatról történő azonnali leválasztásáról, egyúttal a HelpDesk értesítéséről. A számítógépet ilyen esetben nem szabad kikapcsolni és a csatlakoztatott hordozható adattárolókat eltávolítani.

17. Elérhetőségek

A tájékoztatóban felsorolt biztonsági szabályokra vonatkozó kérdésekben az alábbi szervezetek állnak rendelkezésre.

Információ- és adatvédelem:
e-mail: informaciovedelem@mav.hu
Infokommunikációs biztonság:
e-mail: MVZ_IKI_Biztonsag@mav.hu
HelpDesk:
Tel.: 40-00, e-mail: helpdesk@mav-szk.hu