Utasítások

23/2014. (II. 12. MÁV-START Ért. 9.) sz. vezérigazgatói utasítás a MÁV-START Zrt. Informatikai Biztonsági Szabályzata

A MÁV-START Zrt. szervezeteinek és munkavállalóinak informatikai biztonsággal összefüggő feladatait a *2012. évi C. tv.* a Büntető Törvénykönyvről vonatkozó rendelkezései, az *MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.* c. szabvány, *MSZ ISO/IEC 27002:2007 – Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve.* c. szabvány továbbá a *MÁV-START Vasúti Személyszállító Zrt. biztonsági stratégiája* alapján a következők szerint határozom meg.

1.0 AZ UTASÍTÁS CÉLJA

Jelen szabályzat az informatikai biztonság sajátos eszközeivel támogatást kíván adni a MÁV-START Zrt. – továbbiakban Társaság – üzleti céljainak eléréséhez. El kívánja érni, hogy csak olyan informatikai rendszereket, berendezéseket és eljárásokat lehessen alkalmazni, amelyekkel az üzleti folyamatok biztonságosan végezhetők, és amelyek lehetővé teszik a Társaságnak a többi európai vasúttal való zavartalan együttműködését.

2.0. AZ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT HATÁLYA

2.1. A szabályzat hatálya

2.1.1. Az Informatikai Biztonsági Szabályzat személyi hatálya kiterjed:

a) a Társaság Szervezeti és Működési Szabályzatában foglalt valamennyi szervezeti egységre, továbbá valamennyi, az informatikai infrastruktúra működésében vagy használatában érintett munkavállalójára,
b) a Társaság részére informatikai szolgáltatást (üzemeltetés, alkalmazásfejlesztés, eszközbeszerzés, stb.) végző külső cégektől a Társaságunkkal való együttműködésben résztvevőkre, akiknek a Társaság részére vagy eszközeivel végzett munkájában legalább a jelen utasításban foglaltakkal megegyező, és azzal jó összhangban álló védelmi elveket kell érvényesíteni.

2.1.2. Az Informatikai Biztonsági Szabályzat tárgyi hatálya kiterjed:

a) a Társaságnál gyűjtött, felvételezett, továbbítás alatt álló, feldolgozás alatt levő, feldolgozás során létrejött és a tárolt (a továbbiakban: kezelt) információkra, az adatkezelés teljes folyamatára (adat),
b) a Társaságnak az a) pont szerinti adatok kezelését lehetővé tevő összes számítógépes információs rendszerére, alkalmazására, a lehetséges mértékig a rendszerszoftverre is azok teljes életciklusában (szoftver), valamint ezek dokumentációjára,
c) a Társaság tulajdonában lévő, illetve általa használt azon informatikai berendezésekre, elektronikus eszközökre és adathordozókra, amelyek használatával az a) pont szerinti adatok kezelését végzik (hardver).

2.2. A szabályzat kidolgozásáért és karbantartásáért felelős

A szabályzat kidolgozásáért és karbantartásáért a Társaság biztonsági vezetője felelős.

3.0. FOGALMAK MEGHATÁROZÁSA

3.1. Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek, vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

3.2. Adatbázis: azonos minőségű (jellemzőjű), többnyire strukturált adatok összessége, amelyeket tárolásra, lekérdezésre, feldolgozásra, és szerkesztésre alkalmas szoftver kezel.

3.3. Adatállomány: az egy nyilvántartó rendszerben kezelt adatok összessége.

3.4. Adathordozó: a papír és azok a számítógépes alkatrészek, eszközök, amelyekre a munkához szükséges adatokat menteni, tárolni lehet, illetve a hordozható változataikkal gép-gép között adatot lehet cserélni, például:

- mágneses elven működő egységek (pl.: FDD, HDD, IBM Microdrive),

- optikai adattárolás elvén működő adathordozók (pl.: CD, DVD, Blu-ray Disc (BD)),
- memóriakártyák (pl.: Smart Media, Compact Flash, SDHC),
- USB, soros, IRDA portra csatlakoztatható eszközök (pl.: pen drive, okostelefon, fényképezőgép, zenelejátszók, videokamerák).

3.5. Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása, megsemmisítése és tönkremenetele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere (a védelem tárgya az adat).

3.6. Adatvagyon: az adatok és informatikai rendszerek olyan értéke, ami azt fejezi ki, hogy milyen költséget jelent egy rendszer teljes helyreállítása annak összeomlása vagy megsemmisülése esetén. Az adatvagyont rendszerenként kell megállapítani és Társaságra összegezni.

3.7. Adatvédelem: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége. A Társaságnál folytatott adatkezelések szabályait az Adatvédelmi Szabályzat rögzíti.

3.8. Alkalmazás: minden olyan szoftver, amely (akár egy, akár több felhasználó által) az informatikai eszközön futtatható, és nem az operációs rendszer szerves része. Ilyen szoftver, program például a GIR, a SZVÖRNET, amely a felhasználó a munkáját segíti, vagy ahhoz szükséges információkat gyűjt, rendszerez, tárol, kezel.

3.9. Auditálás: a Társasági gyakorlat és rendszer összehasonlítása azokkal a pontosan meghatározott jogszabályokkal, hatósági előírásokkal, belső utasításokkal, módszerekkel, eljárásokkal, amelyek értelmében előírásszerűen működnie kell.

3.10. Belső adat: a Társaság tevékenységéhez kapcsolódó olyan adat, amelynek a védelméhez méltányolható érdek fűződik, és nyilvánosságra kerülése sértené a Társaság érdekeit, de az üzleti titok kategóriába nem sorolható, annál kevésbé fontos tartalommal bír.

3.11. Bizalmasság: az adat azon tulajdonsága, hogy védett illetéktelen hozzáférés, illetve felhasználás ellen. Annak biztosítása, hogy az információkhoz, adatokhoz csak az arra jogosítottak, csak az előírt módokon és csak célhoz kötötten férhessenek hozzá.

3.12. Biztonsági osztály: az informatikai rendszer biztonsági követelményeire jellemző kategória, aminek alapja az adatok fontossága, értéke, titokká minősített volta, stb., a sérülésükből és kiesésükből eredő károk nagysága. A biztonsági követelmények a biztonsági osztálytól függőek, és az osztályok szerint rendre emelkedő szintű biztonságot definiálnak. Három kategóriát: alap - fokozott – kiemelt különböztetünk meg mind az információvédelem (bizalmasság és sértetlenség együtt), mind pedig a rendelkezésre állás területén.

3.13. Biztonsági esemény: a biztonságot fenyegető egy vagy több tényező tényleges fellépése, bekövetkezése illetve jelentkezése.

3.14. BYOD (Bring Your Own Device): „Hozd a saját eszközödet” irányzat, amely a saját tulajdonú (általában hordozható) eszközökön történő munkavégzést jelenti vállalati környezetben.

3.15. Elektronikus aláírás: elektronikus dokumentumok, adatok hitelesítésére szolgáló, a dokumentumból matematikai algoritmussal készített kódsorozat, amit a hitelesíteni kívánt üzenetek végéhez csatolnak, és azzal együtt továbbítanak. Lehetővé teszi, hogy az üzenet olvasója ellenőrizni tudja egyrészt az üzenetet küldő személyazonosságát, másrészt az üzenet sértetlenségét. A küldő privát kulcsával készül és annak publikus kulcsával lehet ellenőrizni eredetiségét. Egyszerű, fokozott biztonságú és minősített kategóriája létezik.

3.16. Erőforrás-kihelyezés (kiszervezés, outsourcing): egy társaság valamely informatikai területének, tevékenységének, sőt gyakran eszközeinek vagy munkatársainak a kihelyezése egy külső vagy belső szolgáltató szervezethez úgy, hogy a kihelyező előre meghatározott és folyamatosan mért minőségű szolgáltatást kap, előre meghatározott áron és feltételek mellett. Az elvárt szolgáltatási szintet és minőséget, nem megfelelő szolgáltatás esetén a szolgáltatót terhelő kártérítési kötelezettséget, egyéb feltételeket szolgáltatási szint megállapodásban (Service Level Agreement, SLA) rögzítik.

3.17. Érzékeny adat: a személyes adat és a titokká minősített adat együttes elnevezése.

3.18. Felhasználó: az az alkalmazott, aki informatikai eszközt és programot (alkalmazást) használ munkaköri feladatai megoldásához, aminek teljesítéséhez – a szükséges szabályok elfogadását követően – az eszközök és az alkalmazás használatára használati (hozzáférési) jogosultságot kapott.

3.19. Fenyegető tényezők: olyan események vagy körülmények, amelyek következtében az informatikai rendszerelemek bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, így fellépésük kedvezőtlen következményekkel járhat, illetve veszteséget, kárt okozhat, vagy egyéb hátrányos hatást gyakorolhat. Ezek lehetnek személyektől eredő támadások, események (adatbeviteli hiba, hibás kezelés), véletlen események (pl. áramkimaradás), külső tényezők (pl. tűzeset) általi behatások és olyan körülmények, amelyek magának az informatikának a sajátosságaiból fakadnak (hardver tönkremenetele, kártékony program, vírus, programhiba, stb.).

3.20. Gyenge pont: az informatikai rendszerelem azon jellemzője, hiányossága, amelynek révén az a fenyegető tényezők hatásának van kitéve.

3.21. Hitelesség: a rendszerben kezelt adatnak az a tulajdonsága, hogy bizonyíthatóan a megjelölt forrásból származik, azaz a kapcsolatba kerülő rendszerelemek kölcsönösen és egyértelműen azonosítják egymást, és ez az állapot a kapcsolat teljes idejére fennmarad.

3.22. Hozzáférési jogosultság: az informatikai rendszerben elvégezhető tevékenységekre vonatkozó engedély a felhasználó számára.

3.23. Informatikai biztonság: az informatikai infrastruktúra olyan működési és védelmi állapota, amely a megfelelő erőkkel, eszközökkel és módszerekkel akadályozza a veszélyhelyzetek kialakulását, veszélyhelyzetben pedig garantálja a várható vagy már meglevő káros hatások csökkentését, semlegesítését, a kiesett rendszer vagy rendszerelemek pótlását. Célja, hogy a rendszer védelme – az általa kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából – zárt, teljes körű, folyamatos és a kockázatokkal arányos legyen. Az informatikai biztonság aktuális szintje a vonatkozó előírások, szabványok betartásának vagy mellőzésének az eredménye, pillanatnyi dinamikus állapot a fenyegetettség és a védelem között.
Biztosítja, hogy az adat védett legyen a jogosulatlan felhasználók által történő megismerés ellen (bizalmasság), az információk jogosulatlanok általi módosítása ellen (sértetlenség), valamint biztosítja a jogosultak számára térben és időben a szükséges hozzáférést (rendelkezésre állás).

3.24. Informatikai biztonsági szabályzat, IBSZ: a kibocsátó összes szervezeti egységére és munkatársára szabályokat tartalmazó dokumentum, aminek tartalma a biztonságpolitika rögzítése, és az abban kinyilvánított célok és biztonsági alapelvek alapján történő működési rend és mód részletes meghatározása. Kiterjed különösen a fizikai és személyi környezethez, a hardver- és szoftverrendszerhez, a kommunikációhoz és a számítógépes hálózathoz, az adathordozókhoz, a bemenő és kimenő adatokhoz, továbbá a dokumentációhoz kapcsolódó biztonsági szabályokra. Alapul szolgál a Rendszerszintű Informatikai Biztonsági szabályzat (RIBSZ) számára.

3.25. Informatikai Működésfolytonossági Terv (IMFT): terv arra, hogy ha az informatikai rendszer rendelkezésre állása az elviselhető kiesési időn túl akadályozott, az esetleg sérült rendszerösszetevők és szolgáltatások helyreállíthatóak, illetve másik környezetben – akár csökkentett terjedelmű szolgáltatással – újraéleszthetőek legyenek.

3.26. Intranet: belső, csak egy adott szervezet informatikai eszközeinek felhasználói által elérhető hálózat, amiben a felhasználó az elérhető adatokat olyan kezelői felületen („böngésző”) látja, mint ha azok az Internetről érkeznének. Ehhez az adatokat – Word vagy Excel formátumból, adatbázisból, stb. – előzetesen át kell alakítani a böngészőprogram által érthető formátumúra. Az Intranet hálózatot védeni kell külső – a Társasághoz nem tartozó – felhasználók, káros programok, stb. bejutása ellen.

3.27. ITIL (IT Infrastructure Library): az 1980-as években, Angliában több, információtechnológiával (IT) foglalkozó cég által a brit

kormány támogatásával létrehozott dokumentumsorozat, amiben az üzleti folyamatok IT eszközökkel megvalósított támogatására a gyakorlatban alkalmazott, jól bevált, gyártótól független üzemeltetési ajánlásokat gyűjtötték össze. Jelenleg a harmadik verziónál tart, 5 fő kötetből, és az ezekhez kapcsolódó kiegészítő anyagokból áll. Az ITIL a leginkább használt megközelítés az IT szolgáltatás-menedzsmentre, és főképp Európában az üzemeltetés de facto szabványa. Kizárólag az informatika üzemeltetési és üzemeltetés-szervezési kérdéseivel foglalkozik, dokumentált, kidolgozott oktatási és vizsgarendszere van.

3.28. Jogtiszta szoftver: olyan számítógépes program – alkalmazás – amelynek használatára a használó (jellemzően vásárlással, eseti megállapodással, ritkábban ajándékozással, stb.) megszerezte a jogosultságot. Általában ahány felhasználó kívánja a szoftvert egyidejűleg használni, annyi számú használati jogosultságot (liszensz) kell megszerezni, de más konstrukciók is léteznek (függhet pl. a telepítések darabszámától, a gépek számától, a processzorszámtól, stb.)

3.29. Katasztrófa: egy meghatározott területen vagy létesítményben bekövetkező, természeti erő vagy emberi tevékenység következtében létrejött esemény (beleértve a súlyos balesetet is), ami a felhasználó életét és/vagy egészségét, az informatikai infrastruktúrát vagy a környezetet olyan súlyosan veszélyezteti vagy károsítja, hogy következményeinek mérséklése és felszámolása rendkívüli intézkedéseket igényel. A katasztrófa az informatikai biztonsági események legsúlyosabb előfordulása, ami a megengedett kiesési időnél hosszabb időszakra megakadályozza, vagy megszűnteti a rendszer teljes egészének vagy tevékenységei / szolgáltatásai jelentős részének a folyamatos működését.

3.30. Kockázat: olyan fenyegető tényező vagy esemény bekövetkeztének az esélye, amely hátrányosan érintheti a Társaság informatikai rendszerének a működését. Elemei: a bekövetkezés gyakorisága és kárnagyság. A kockázatot elemzéssel, a rendszert fenyegető tényezők azonosítása és veszélyességük értékelése útján kell megállapítani.

3.31. Kockázatkezelés: az a döntési és cselekvési folyamat, amelynek során az üzleti tulajdonosok felmérik és minősítik informatikai rendszerük biztonsági kockázatait, és védelmi eszközöket rendelnek azok mellé. Ésszerű egyensúlynak, arányosságnak kell fennállnia a biztonsági intézkedések költsége és azon kockázatok között, amelyeket ezekkel az intézkedésekkel csökkenteni szándékoznak.

3.32. Kritikus rendszer: olyan informatikai rendszer, amely a Társaság számára alapvető fontosságú az üzleti folyamatok viteléhez, és a működéshez a Társaságnak elemi érdeke fűződik.

3.33. Közvetlen vezető: aki a Társaság által biztosított informatikai eszközt, e-mail címet használó munkatárs munkáját irányítja.

3.34. Különleges személyes adat: (A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Infotv.) által különleges adatként meghatározott személyes adatok köre.)
a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

3.35. LAN, WAN: számítógépes hálózat, ami topológiáját tekintve lehet helyi méretű (LAN, Local Area Network) vagy szélesebb területet érintő (WAN, Wide Area Network).

3.36. Maradványkockázat: az a – rendszerint kismértékű – kockázat, ami annak ellenére fennmarad, hogy a fenyegető tényezők ellen intézkedéseket tettünk, illetve az a kockázat, ami ellen valamilyen okból (alacsony várható kárnagyság, igen ritka jelentkezés, forráshiány, stb.) nem tervezünk ellenintézkedést.

3.37. Minősített informatikai rendszer: olyan informatikai rendszer, amely fokozott vagy kiemelt biztonsági osztályú besorolást kapott (pl. azért, mert érzékeny adatot kezel, tárol, dolgoz fel, vagy azért, mert kritikus fontosságú a Társaság üzletvitele szempontjából).

3.38. Modem MOdulator/DEModulator: a digitális jeleket analóg telefonhálózatokon való átvitelhez át- és visszaalakító hardver eszköz.

3.39. Mobil kommunikáció: a különböző szolgáltatók által az országos GSM hálózaton keresztül végzett mindennemű hang, adat és információ átvitel.

3.40. Operációs rendszer: a szerverek, munkaállomások, PC-k, stb. működését alapvetően meghatározó és azt biztosító szoftver (rendszer), a számítógép alkalmazói programok nélküli „tudása”.

3.41. QR-kód: kétdimenziós vonalkód (pontkód), az angol *Quick Response* (=*gyors válasz*) rövidítése. A QR-kód nyílt szabványú, a specifikációi nyilvánosak, ISO/IEC 18004 jelzettel nemzetközi szabvánnyá vált, amit 2006-ban kiegészítettek. Bármilyen irányból olvasható, nem kell törődni a kód helyes tájolásával. A QR-kódokban nyílt és rejtett szövegek, Internetes címek, azok leolvasásakor azonnal futtatható programsorok, utasítások, stb. helyezhetők el.

3.42. Rendelkezésre állás: a rendszernek az a tulajdonsága, hogy meghatározott helyen és időben (pl. az összesített havi üzemidő 98 %-ában) az eredeti rendeltetésének megfelelő szolgáltatásokat nyújtani tudja.

3.43. Rendszeradminisztrátor – rendszergazda: az informatikai rendszer telepítését, konfigurálását, karbantartását munkaköri feladatként végző, az ehhez szükséges speciális ismeretek és a felhasználóénál bővebb rendszer-hozzáférési engedélyek birtokában levő személy.

3.44. Rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, a rendszerben kezelt adatok mentését, a meghibásodott rendszer helyreállítását munkaköri feladatként végző, az ehhez szükséges speciális ismeretek és a felhasználóénál bővebb rendszer-hozzáférési engedélyek birtokában levő személy.

3.45. Rendszerszintű Informatikai Biztonsági Szabályzat, RIBSZ: az Informatikai Biztonsági Szabályzat szerkezetét és követelményeit alapul véve az adott informatikai rendszerre nézve specifikus szabályokat tartalmazó dokumentum.

3.46. Sértetlenség: az adatok eredeti állapotának, tartalmának, teljességének és hitelességének biztosítása. Célja, hogy az információkat, adatokat, programokat csak az arra jogosultak (személyek, vagy más rendszer-összetevők) változtathassák meg, és azok véletlenül se módosuljanak. A sértetlenség megtartása az illetéktelen módosítás, hamisítás elleni védelmet is jelenti.

3.47. Számítási felhő (cloud computing): a felhő alapú számítástechnikai szolgáltatás olyan szolgáltatás, amelyet a szolgáltató a felhasználó számára nem egy erre a célra rendelt hardvereszközön, hanem a saját eszközein elosztva, az üzemeltetés részleteit elrejtve üzemelteti, és amelyet a felhasználók az Interneten, vagy a vállalati Intraneten keresztül érhetnek el. Az erőforrások nagysága, szerkezete, összeköttetése nem ismert - innen a felhő elnevezés. Az állományok egy vagy több központi szerveren tárolódnak, a felhasználók kliens programokkal (pl. böngésző) férnek hozzá az adataikhoz. Ugyan azokon az erőforrásokon több igénybe vevő is osztozik. A felhasználók igény szerinti hozzáférést kapnak a megosztott informatikai erőforrásokhoz (pl. hálózat, szerverek, tárolók, alkalmazások és szolgáltatások).
A kialakítás szerint lehet:

- Privát: belső szolgáltató által egy zárt intézményi kör számára nyújtott felhő szolgáltatatás,
- Publikus: egy nyilvános szolgáltató által nyújtott,
- Hibrid: Vegyesen a belső szolgáltató által és publikus szolgáltatótól is igénybe vett kapacitásokat használ.

3.48. Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés.
A személyes adatok kezelésének rendjét a Társaság vezérigazgatói utasításként hatályba lépett Adatvédelmi Szabályzata tartalmazza.

3.49. Titokká minősített adat: olyan adat, amely törvényi rendelkezés alapján nemzeti minősített adat (Szigorúan titkos, Titkos,

Bizalmas, illetőleg Korlátozott terjesztésű), illetve a Társaság Üzletititok-védelmi Szabályzata alapján az üzleti titok körbe tartozik, nem ideértve az ún. belső adatot.

3.50. Ügyfél: az utas, az utazás előkészítése, helyfoglalás, stb. érdekében a nyilvános online rendszereken (e-Ticket, ELVIRA, stb.) a Társasághoz forduló, a Társaság ügyfélszolgálatától információt kérő vagy ott bejelentést, panaszt tevő személy, továbbá a Társaság által üzleti ajánlattal megkeresett, és a kedvezményes utazásra jogosító igazolvánnyal ellátott személy.

3.51. Üzleti titok: üzleti titoknak minősül a Társaság gazdasági, üzleti tevékenységéhez kapcsolódó vagy annak során keletkező minden adat, amelynek titokban maradásához a Társaságnak méltányolható érdeke fűződik, nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a Társaság jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, és amelynek titokban tartása érdekében a Társaság a szükséges intézkedéseket megtette. Üzleti titoknak minősül továbbá minden harmadik félre vonatkozó olyan adat, amelyre nézve a Társaságot jogszabály vagy szerződés alapján titoktartási kötelezettség terheli.

Az üzleti titok minősítésű adatok kezelésének rendjét a Társaság vezérigazgatói utasításként hatályba lépett Üzletititok-védelmi Szabályzata tartalmazza.

3.52. Üzleti tulajdonos: az információs rendszer üzleti tulajdonosa az a – lehetőleg – magasabb beosztású vezető, akinek jogában áll a rendszer fejlesztésével, beszerzésével, használatával és karbantartásával kapcsolatos döntéseket meghozni. Célszerűen az a szervezeti egységi vezető, akihez az adott rendszer felhasználóinak többsége tartozik. Az informatikai biztonsági szempontok szerint értelmezett „tulajdonos” felelőssége kiterjed az adott rendszer informatikai termékeit, illetve szolgáltatásait érintő hagyományos és számítógépes feldolgozás biztonsága érdekében hozott valamennyi intézkedésre. Ő a rendszer biztonsági kockázatainak kezelője, de megbízottakat nevezhet ki, akik a nevében eljárnak. Ugyanazon személy egyszerre több rendszernek is lehet az üzleti tulajdonosa. A MÁV csoport által közösen használt rendszerek esetében (pl. GIR, IHIR) az üzleti tulajdonos felelőssége csak a Társaság által használt modulra terjed ki, feladatai e körre szűkítve értelmezettek.

3.53. Tűzfal: olyan hálózati berendezés vagy program, amely rendszerint a külső Internet-kapcsolat és a céges belső számítógépes hálózat közé illesztve egyrészt védi a hálózatot és rajta működő eszközöket az illetéktelen külső behatolási kísérletektől, másrészt intézi a legális adatforgalmat. Tűzfal alkalmazható továbbá egy adott alkalmazás és a társasági intranet közötti kapcsolat biztonsága érdekében, vagy például személyes tűzfalként egy munkaállomás és teljes külvilág közötti adatkapcsolati kockázatok csökkentésére.

3.54. Változáskezelés: azon szabályok összessége, amelyek meghatározzák egy informatikai alkalmazás adatszolgáltatási folyamataiban, az azokat kiszolgáló informatikai eljárásokban és szolgáltatásokban, valamint az alkalmazás üzemeltetését lehetővé tevő informatikai infrastruktúrában bekövetkező módosítások, változások biztonságos végrehajtását és nyilvántartását, változásainak nyomon követhetőségét.

3.55. VPN: (Virtual Private Network – virtuális magánhálózat): Olyan virtuális számítógépes hálózat, amely kommunikációs csatornák és eszközök segítségével valósul meg, de az azokon zajló egyéb forgalomtól elkülönülő, mások számára nem hozzáférhető egységet képez. A VPN az adatok védelmére, a hitelesítés mellett, nyilvános hálózatokon különböző titkosítási technikákat is alkalmaz, miáltal lehetőséget biztosít a Társaság számára, hogy a belső hálózat meghatározott elemeit elérhetővé tegye az erre feljogosított (pl. zárt felhasználói csoport, illetve távmunkát végző) felhasználók számára.

4.0. UTASÍTÁS LEÍRÁSA

4.1. A MÁV-START Zrt. információbiztonsági politikája

A Társaság informatikai rendszerei által kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítására irányuló tudatos védelempolitikának és az ennek érvényesítésével folytatott tervszerű, egységes és megelőző (pro-aktív) szemléletű biztonsági

tevékenységnek az alábbi védelmi alapelveken kell nyugodnia.

a) Az Informatikai Biztonsági Szabályzatban meghatározott előírás, feladat, magatartási szabály – munkakörre, beosztásra való tekintet nélkül – kötelező érvényű. A szabályzatban foglaltak nem megfelelő végrehajtása vagy be nem tartása a Társaság részéről munkáltatói intézkedést, kártérítési eljárást, törvénybe ütköző súlyosságú esetekben pedig szabálysértési vagy büntetőeljárást vonhat maga után.

b) Minden vezető felelős az informatikai biztonsági szabályzatban foglaltak végrehajtásáért az általa irányított szervezeti egységnél. Azon vezetőknek, akiknek számítógépet használó munkatársaik vannak, biztosítaniuk kell, hogy az információbiztonsági politikát és szabályokat minden munkavállaló megismerje, munkája során alkalmazza, továbbá a felügyelete alatt álló informatikai infrastrukturális elemen vagy elemmel munkát végző külső (nem a Társaság alkalmazásában álló) munkatársakkal betartassa.

c) Minden informatikai eszközt használónak tudatában kell lennie, hogy személyesen felelős az információvédelmi szabályok megismeréséért, saját munkájában azok betartásáért, melyről írásban nyilatkozik.

d) A Társaság minden munkavállalója köteles a biztonsági szabályokat, előírásokat, technikai megoldásokat, beállításokat belső adatként kezelni. Ezeket az információkat külső fél részére csak a Biztonság engedélyével lehet kiadni.

e) A védelmet fizikai, logikai és adminisztratív vonatkozásban egyaránt érvényesíteni kell az összes rendszerelemre (teljes körűség).

f) Szerves egységet alkotó, az összes valószínűsíthető fenyegetés elleni védelmi intézkedési rendszert kell megvalósítani az informatikai infrastruktúra védelmére (zártság).

g) Az informatikai rendszerek és az általuk kezelt adatok védelme erősségének és költségeinek a felmért kockázatokkal arányosnak kell lennie (kockázatarányosság).

h) Az informatikai rendszerek védelmét az információvédelem (bizalmasság és sértetlenség együtt) és a rendelkezésre állás szempontjai szerint megállapított biztonsági osztálya (alap, fokozott, vagy kiemelt) alapján kell megvalósítani (differenciált védelem elve).

i) A védelemben biztosítani kell a tervezés – megvalósítás – ellenőrzés – beavatkozás folyamatát (zárt szabályozási ciklus alapelve).

j) Szét kell választani a tevékenységeket, a feladatokat és a felelősségi köröket a rendszerek fejlesztése, használatba vétele, működtetése és felhasználása terén.

k) Az informatikai rendszerek fejlesztése és megvalósítása során kialakított védelmi képességeket a rendszer teljes életciklusában fenn kell tartani (folytonosság).

l) Új rendszerek / rendszerkomponensek használatba vételével az informatikai biztonság meglévő szintje nem csökkenhet. A fejlesztés során az informatikai biztonság rendszerszintű megtervezésével a fejlesztési igény megjelenésétől kezdve foglalkozni kell.

m) A rendszerekben megvalósított hozzáférésnek és a rendszer használatának a funkcionális szükségszerűségen kell alapulnia. A felhasználók különböző rendszerekhez való hozzáférési jogosultságait a lehetőség szerinti legalacsonyabb szinten kell tartani (szükséges minimális jogosultság elve).

n) A Társaság számítástechnikai rendszereiben kizárólag jogtiszta szoftverek vezethetők be és üzemeltethetők.

o) A munkakör ellátásához kapott, a Társaság tulajdonát képező informatikai eszköz (PC, laptop, hordozható eszközök, nyomtató, szoftver, stb.) kizárólag a munka és az azzal összefüggő elektronikus kommunikáció végzésére szolgál, magáncélú használata (pl. az ún. közösségi hálózatok – Facebook, Skype, stb. – látogatása) nem megengedett. Az eszközök szabályszerű használatát a Társaság esetenként ellenőrzi.

p) A Biztonság szervezetén belül létrehozott információbiztonsági területet minden olyan fejlesztésbe kötelező bevonni, ami informatikai vagy infokommunikációs jellegű, a társaság informatikai eszközeivel, azok bővítésével, selejtezésével, a központi informatikai rendszerben történő változásokkal foglakozik.

q) A Társaság informatikai rendszerében saját eszközöket használni tilos, az ún. BYOD-t a Társaság nem támogatja.

r) A Társaság alkalmazásai, adatbázisai nem működhetnek cloud (felhő) alapú technika alkalmazásával.

s) A felhasználók kötelesek alkalmazni az 1. sz. mellékletbe foglalt használati szabályokat,

amelyek megismerését a 3. sz. melléklet szerinti nyilatkozattal kell igazolniuk. Ennek kitöltéséről a 4.4.1. Informatikai biztonsági követelmények érvényesítése alpont rendelkezik.

4.2 A MÁV-START Zrt. informatikai biztonságának szervezeti struktúrája

A Társaság informatikai infrastruktúrája biztonságának központi irányítását a vezérigazgató gyakorolja. A szakmai irányítás és felügyelet az SZMSZ-ben foglaltak szerint a Biztonság, azon belül az információvédelmi szakterület útján valósul meg.

4.2.1. A Társaság informatikai biztonságát irányító vezetők és biztonsági feladataik

a) Vezérigazgató

A felsőszintű központi irányítás keretében az alább felsoroltakat végzi.

- Létrehozza a Biztonság szervezetén belül az információbiztonság munkaszervezetét, és azon belül meghatározza az alapvető létszámnormákat.
- Jóváhagyja a Társaság biztonsági stratégiáját, ezáltal meghatározza az annak részét képező informatikai biztonsági működés elveit.
- A Társaság gazdálkodása útján biztosítja a hatékony működés szervezeti, anyagi, műszaki, személyi, tárgyi feltételeit.
- Vezérigazgatói utasításként kiadja a Társaság Informatikai Biztonsági Szabályzata (IBSZ) c. (jelen) dokumentumot.
- Az információvédelmi munkaszervezet útján irányítja és ellenőrzi a Társaság informatikai biztonsági tevékenységét.
- Meghatározza az informatikai biztonsági oktatás, képzés, továbbképzés elveit.

b) Biztonsági vezető

- Intézkedik a Társaság informatikai biztonságát meghatározó szabályozási feladatok szakszerű, a jogszabályoknak megfelelő előkészítésére.
- Szabályozza az informatikai biztonsági tevékenység szakmai és a munkafolyamatokba épített ellenőrzési feladatait, tevékenységét.
- Munkaszervezetének információvédelmi szakterülete útján biztonsági szempontból felügyeli a Társaság Informatika szervezetének munkáját.
- Értékeli a szervezeti egységek informatikai biztonsági helyzetét, segíti informatikai biztonsági tevékenységüket.
- Szükség esetén informatikai biztonsági intézkedést, állásfoglalást, körlevelet, stb. ad ki, és végrehajtását az információvédelmi szakterület útján rendszeresen ellenőrzi.
- Bűncselekmény elkövetésének megakadályozására, a Társaságot veszélyeztető károkozás megelőzésére, illetve az ilyen károk csökkentése érdekében intézkedik az érintetteknek az informatikai rendszerekből való kizárására.
- Azonnali intézkedéseket rendel el az információbiztonság sérülése, vagy ennek veszélye esetén.
- Hatóságoknál informatikai biztonsági kérdésekben képviseli, vagy képviselteti a Társaság érdekeit.

c) Biztonság információbiztonsági koordinátora

Felelős:
- a Társaság szervezeti egységeinél folyó informatikai biztonsági tevékenység irányításáért, felügyeletéért, koordinálásáért,
- a Társaság informatikai biztonsági stratégiájának kialakításáért,
- az információbiztonsági szabályozás megfelelőségéért, az IBSZ kialakításáért, évenkénti (az informatikai infrastruktúrában bekövetkező jelentős változás esetén soron kívüli) felülvizsgálatáért és szükség szerinti aktualizálásáért,
- az információbiztonsági veszély- és kármegelőzésnek, a biztonsági ellenőrzés és vizsgálat módszereinek, eljárásainak megfelelőségéért, szakszerűségéért,
- az informatikai szolgáltatók és szolgáltatási szerződések biztonsági megfelelőségének ellenőrzéséért,
- az adat- és információbiztonsági oktatás, képzés és tanácsadás szakmai irányításáért, a vezetők és munkatársak biztonsági tudatának fejlesztéséért,
- az informatikai rendszerek és rendszeradminisztrátorok folyamatos biztonsági felügyeletéért,
- a biztonsági események kivizsgálásáért, értékeléséért,
- a veszélyeztetés-felmérés, kockázatelemzés, kárelhárítás és kármérséklés tervezésének irányításáért.

Feladata:
- jelen szabályzatban megfogalmazott követelmények betartását ellenőrzi, a hiányosságok megszűntetésére intézkedik,
- segíti az üzleti tulajdonosokat a biztonsági szaktevékenység előírásszerű ellátásában,
- ellenőrzi a biztonsági folyamatok tervezését, a társasági szintű szabályozások kialakítását, azok betartását,
- biztonsági szempontból felügyeli az informatikai fejlesztéseket,
- koordinálja az informatikai rendszerek üzemeltetésének biztonságát,
- koordinálja, ellenőrzi az outsourcing partnerek által a Társaság részére végzett informatikai biztonsági tevékenységeket,
- információbiztonsági ellenőrzéseket végez a Társaság szervezeti egységeinél,
- együttműködik a Társaság munkaszervezeteivel az informatikai biztonság továbbfejlesztése érdekében,
- azonnali intézkedéseket rendel el az információbiztonság sérülése, vagy ennek veszélye esetén,
- bűncselekmény elkövetésének megakadályozására, a Társaságot veszélyeztető károkozás megelőzésére, illetve az ilyen károk csökkentése érdekében intézkedik az érintetteknek az informatikai rendszerekből való azonnali kizárására,
- kapcsolatot tart a MÁV-csoporthoz tartozó társ informatikai biztonsági szervezetekkel,
- képviseli a Társaságot a felügyeleti hatóságokkal, igazgatási, rendészeti és más külső szervekkel folytatott tárgyalásokon.

Hatásköre:
- részvétel a társasági szintű informatikai stratégia kialakításában,
- azonnali intézkedések elrendelése az információbiztonság sérülése, vagy ennek veszélye esetén,
- az információvédelmi oktatás követelményeinek, tematikájának és programjának meghatározása, részvétel a képzések megtartásában,
- információbiztonsági ellenőrzések kezdeményezése,
- a Társaságnál kiadásra kerülő szabályzatok véleményezése az informatikai biztonság szempontjai szerint,
- a Társaság szervezeti egységei részére fejlesztett és üzemeltetett informatikai rendszerek információbiztonságának ellenőrzése,
- az informatikai rendszerekben előforduló biztonsági események értékelése alapján meghozandó védelmi intézkedések, szankciók, kezdeményezése, a szükséges intézkedések és tájékoztatások megtétele.

4.2.2. A Társaság informatikai biztonságát megvalósító személyek és biztonsági feladataik

a) Informatikai vezető

Felelős:
- a Társaság informatikai stratégiájának kialakítása és végrehajtása során a jelen IBSZ-ben foglalt előírások érvényesüléséért,
- jelen IBSZ biztonsági követelményeinek megfelelő információvédelmi rendszerek, eszközök beruházásának előkészítésért, beszerzésének irányításáért,
- az üzleti tulajdonosok kijelöléséért, ha az nem lehetséges, utólagos megnevezéséért, azok felelősségi körébe tartozó rendszerek, alkalmazások meghatározásáért,
- az üzleti tulajdonosok személyében előállt változások követéséért, és a bekövetkezett változásokról a Biztonság részére történő legalább évente egyszeri tájékoztatásért,
- annak biztosításáért, hogy új informatikai rendszerek megvalósítást célzó projektek előkészítése során a biztonsági rendszer tervezéséhez és megvalósításához szükséges anyagi, eszköz- és humán feltételek betervezésre kerüljenek,
- annak biztosításáért, hogy az új informatikai rendszerek bevezetésénél, illetve a meglevők korszerűsítésénél a biztonsági rendszer tervezése és létesítése a projektmegvalósítás keretein belül, annak szerves részeként érvényre jusson,
- minden minősített informatikai rendszerre a rendszerfejlesztés részeként a fejlesztést végzővel a rendszerszintű informatikai biztonsági követelmények, a RIBSZ, és az Informatikai Működés-folytonossági Terv kialakíttatásáért,
- informatikai tárgyú beszerzési, szolgáltatási, stb. szerződésekben, továbbá erőforrás-kihelyezéssel működtetett rendszerek esetében a Társaság informatikai biztonsági érdekeinek az érvényesítéséért,
- az informatikai szolgáltatók, szolgáltatási szerződések és SLA-k biztonsági megfelelőségéért,

- a társasági szintű vírusvédelmi rendszer fenntartásáért,
- jogtiszta szoftverekkel való működés feltételeinek kialakításáért, a licenszgazdálkodásért,
- az operációs rendszerek és egyéb rendszerszoftverek biztonsági javításainak telepítéséért,
- a minősített rendszerekben társasági szinten egységesített elvekre (pl. ITIL) épülő változáskezelési eljárásrend kidolgozásáért és működtetéséért,
- a hordozható eszközökkel végzett és a távmunka biztonságos feltételeinek kialakításáért,
- a biztonsági osztályok követelményeinek megfelelő adathálózati védelmi rendszerek és eszközök honosításáért, fejlesztések koordinálásáért, az adathálózatot megvalósító rendszerekben, környezetük minden elemén a zárt és a kockázatokkal arányos védelem biztosításáért,
- a Társaság központi szerverén tárolt adatok, dokumentumok eléréséhez a megfelelő jogosultsági rendszer biztosításáért a szükséges vezetők bevonásával,
- a Társaság informatikai objektumainak, telephelyeinek a fizikai biztonsági követelményeknek megfelelő kialakításáért,
- a Társaság informatikai vagyonleltárának szakmai megfelelőségéért.

b) Humán vezető

Felelős:

– a Társasághoz belépő munkatársak információvédelmi képzésének megszervezéséért,

– a munkaerő-változások során az illetékes humán ügyintéző ellenőrizési és az információvédelmet érintő feladatainak végrehajtásáért és azok ellenőrzéséért (pl. belépőkkel és kilépőkkel az előírt nyilatkozatok aláíratása, belépéskor képzés),

– a kilépett és jogi létszámba került munkatársak hálózati belépési jogosultságának visszavonatásáért az erre kialakított külön szabályok szerint.

c) Számítástechnikai alkalmazás üzleti tulajdonosa

Minden számítástechnikai alkalmazás biztonságát egy-egy üzleti tulajdonoshoz kell rendelni. Az üzleti tulajdonos lehet konkrét személy, de a funkció köthető konkrét beosztás mindenköri betöltőjéhez is.

Felelős:

- a rendszerek tervezése és fejlesztése során az üzemeltetés biztonsági kockázatainak felméréséért és értékeléséért, a kockázatok minimalizálásához szükséges ráfordítások, erőforrások, intézkedések menedzseléséért, a maradványkockázat mértékének meghatározásáért és elfogadásáért,
- az előbbiek alapján a rendszer biztonsági osztályának meghatározásáért egyrészt az információvédelem (bizalmasság és sértetlenség együttesen), másrészt a rendelkezésre állás szerint,
- a rendszer rendelkezésre állási paramétereinek meghatározásáért, a kármérséklési (pl. vagyonbiztosítási) tevékenység irányításáért,
- a rendszer kifejlesztése során a szükséges biztonsági tervek (pl. biztonsági rendszerterv) és okmányok (pl. Informatikai Működésfolytonossági Terv (IMFT)) elkészítéséért,
- a rendszernek a tervekben leírt biztonságú megvalósításáért,
- a rendszer átvétele során a ténylegesen megvalósított biztonság színvonalának ellenőrzéséért és fenntartásáért,
- a kezelt adatok biztonságának az Adatvédelmi Szabályzat és az Üzletititok-védelmi Szabályzat szerinti minősítésének megfelelő szintű biztosításáért az adatok teljes életciklusában,
- az informatikai működésfolytonosság biztosítása érdekében tervezett feladatok gyakoroltatásáért.

Köteles:

- meghozni a rendszer kifejlesztésével (beszerzésével), használatával és karbantartásával kapcsolatos biztonsági döntéseket,
- biztosítani, hogy az informatikai rendszerben valamennyi informatikai biztonsági követelmény teljesüljön, és azokat folyamatosan ellenőrizzék,
- kijelölni a rendszer biztonságos üzemeltetéséhez szükséges közreműködő személyeket,
- a rendszer biztonsági osztályba sorolásából következő védelmi intézkedéseket megtenni, illetve kezdeményezni a Társaság felső vezetése és az informatikai vezető felé,
- a biztonsági előírások érvényesülése szempontjából évente legalább egyszer felülvizsgálni a tulajdonolt rendszer működését biztosító informatikai hátteret, a felhasználókat és jogosultságaikat, továbbá a rendszert használók tevékenységét.

- figyelemmel kísérni a rendszer adataiban és technológiájában történő változásokat, hogy a rendszer adatvagyonát naprakészen ismerje,

Jogosult:
- az esetlegesen előforduló informatikai biztonsági incidensek kivizsgálásában való közreműködésre, a szükséges szankciók kezdeményezésére,
- az információvédelmi szakterület szakmai segítségének közvetlen igénybe vételére.

d) „Felhasználó" beosztottal rendelkező közvetlen vezető

Irányítási területén biztosítania kell, hogy az informatikai biztonságra vonatkozó dokumentumokban (jelen IBSZ, alkalmazásonkénti RIBSZ, IMFT, stb.) foglaltakat minden általa vezetett munkavállaló és külső munkatárs a rá vonatkozó mértékben megismerje és betartsa. Ennek során feladata:
- a közvetlen irányítása alá tartozó munkavállalók részére a szervezetben betöltött munkakörüknek megfelelően az informatikai rendszerhez történő hozzáférés biztosítása, kiemelten jelen utasítás 4.7.1 pontja szerint a hozzáférés folyamatos aktualizálása (felfüggesztetése, újraindíttatása stb.),
- a felhasználói rendszerekhez a szükséges minimumra korlátozott felhasználói jogosultságok biztosítása (igénylés, módosítás, felfüggesztés, visszavonás, stb. kezdeményezése),
- a központi irodaépületben üzemelő vezeték nélküli hálózathoz (WiFi) a felhasználó részére hozzáférés igénylése a biztonsági vezetőtől.
- a működési területén külső személyek által végzett informatikai tevékenységekhez (karbantartás, javítás, stb.) szükséges ideiglenes jogosultságok biztosítása, minősített rendszerek esetén a munkálatok felügyeletének megszervezése,
- a rendszerek használata során észlelt új kockázatok, változtatási igények folyamatos figyelemmel kísérése, a tapasztalható gyenge pontok vagy az esetleg bekövetkező biztonsági események jelzése közvetlen felettese, az adott rendszer üzleti tulajdonosa, és közvetlenül az információvédelmi koordinátor részére,
- szükség esetén a működési területe speciális jellegzetességeit tükröző helyi végrehajtási utasítás kibocsátásának kezdeményezése vezetőjénél az IBSZ, illetve a RIBSZ-ek előírásainak teljesülése érdekében,
- a rendszerek nem biztonságos, a Felhasználók biztonsági kötelezettségei c. okmányban (1. sz. melléklet) rögzítettől eltérő használatának észlelésekor a használat leállítása és az esemény jelentése közvetlen felettese, továbbá az adott rendszer üzleti tulajdonosa, és az információvédelmi koordinátor részére,
- gondoskodik a beosztott munkatársak részére biztosított asztali és hordozható eszközök használatba adásáról, visszavételéről, az eszközök állapotának folyamatos figyelemmel kíséréséről, az eszközök biztonsági állapotában bekövetkezett változások jelentéséről a Biztonság részére.
- A munkatársak munkaviszonyában beállt változások során köteles együttműködni az illetékes humán ügyintézővel.
- a közvetlen irányítása alá tartozó munkavállaló munkaviszonyának bármilyen okból való megszűnésekor a munkavállaló által használt eszközön esetleg tárolt személyes adatok, továbbá postafiókjából a személyes levelek töröltetése úgy, hogy a számítógépen, a központi adattárolásra szolgáló szerver megfelelő könyvtáraiban, és a postafiókban csak azok az állományok maradhatnak, melyek a munkakört a továbbiakban ellátó másik személy munkavégzéséhez szükségesek,
- a közvetlen irányítása alá tartozó munkavállaló munkaviszonyának bármilyen okból való megváltozásakor a munkavállaló által az informatikai rendszerekben (pl. DMS-Poszeidon) kezelt adatokhoz, dokumentumokhoz történő további hozzáférésről gondoskodni köteles,
- a közvetlen irányítása alá tartozó munkavállaló munkaviszonyának bármilyen okból való megszűnésekor a munkavállalónak az általa használt informatikai rendszereket érintő valamennyi felhasználói jogosultsága garantáltan és dokumentáltan letiltásra kerüljön, amit a munkavállaló kiléptető lapján aláírásával kell igazolnia.

A felhasználó beosztottal rendelkező közvetlen vezető informatikai biztonsági jellegű további feladatait részletesen a 13. számú melléklet tartalmazza.

e) Biztonság információvédelmi szakértője

Az információvédelmi szakterület szervezeti keretei között dolgozó információvédelmi szakértők közreműködnek a társasági SZMSZ által a szakterülethez delegált feladatok végrehajtásában, különösen az alább felsoroltakban:

- a rendszerszintű informatikai biztonsági okmányok kidolgozása, illetve kidolgoztatásukban közreműködés,
- közreműködés a társaság Informatikai Biztonsági Szabályzatának kidolgozásában és módosításában,
- informatikai fejlesztésekben az információvédelmi szakterület képviselete,
- az informatikai biztonsági rendszerek, valamint a rendszer-adminisztrátorok, rendszergazdák, és felhasználók – ideértve a rendszergazda jogosultságúakat is – tevékenységének ellenőrzése, biztonsági felügyelete,
- rendszerüzemeltetési okmányok vizsgálata,
- informatikai biztonsági események kivizsgálása,
- javaslattétel a védelmi intézkedésekre, szankciókra,
- a logikai, a fizikai és az adminisztratív biztonság megvalósulásának felügyelete,
- informatikai biztonsági szaktanácsadás, üzleti tulajdonosok, közvetlen vezetők, felhasználók segítése,
- informatikai biztonsági képzés, oktatás.

f) Rendszeradminisztrátor, felhasználói rendszergazda

A hatáskörébe tartozó rendszer(ek) vonatkozásában feladata:

- a logikai védelmi rendszer egyes elemeinek beállítása, módosítása a védelmi rendszertervnek és a RIBSZ-nek megfelelően,
- és a jóváhagyott jogosultságok beállítása, módosítása, aktualizálása a jóváhagyott változásoknak megfelelően.
- Jogosultság kezelési űrlapok kezelése a rendszer teljes életciklusában.

g) Felhasználó

A Társaság minden munkavállalója, aki munkája során számítógéppel adatot gyűjt, feldolgoz és használ (röviden: felhasználó), köteles az ilyen műveletek során az általa kezelt rendszer informatikai biztonságára vonatkozó dokumentumokban foglalt szabályok szerint eljárni. Köteles továbbá a Felhasználók biztonsági kötelezettségei c. okmányban (1. sz. melléklet) foglaltakat ismerni és napi munkájában alkalmazni.

h) Humán ügyintéző

A társaság illetékes humán ügyintézői kötelesek a munkatársak munkaviszonyában beállt változások során ellenőrizni, hogy a munkatárs közvetlen vezetője végrehajtotta-e a rá vonatkozó feladatokat, valamint biztosította-e a közvetlen vezető részére a szükséges információvédelmi dokumentumokat.

i) Biztonság területi biztonsági szakértője

A területi biztonsági szakértő köteles az ellenőrzési tevékenységei során meggyőződni a számítógépek és egyéb informatikai eszközök tárolásának, felhasználásának körülményeiről. Köteles tájékozódni, hogy minden munkatárs a megfelelő jogosultságokkal rendelkezik-e és csak a jogosultságainak megfelelően dolgozik. Bármilyen tapasztalt rendellenesség esetén köteles írásban tájékoztatni az információbiztonsági koordinátort.

4.2.3. Az informatikai biztonság szabályozása a Társaság partnereire vonatkozóan

A Társasággal – az informatikai rendszerek használatával, üzemeltetésével, fejlesztésével összefüggésben – kapcsolatban álló jogi és természetes személyeket, jogi személyiséggel nem rendelkező szervezeteket (továbbiakban: partnereket) érintő tevékenységekben a Társaság informatikai biztonsági érdekeinek és szabályainak érvényre juttatása minden esetben a kérdéses rendszer üzleti tulajdonosának a feladata. A cél az, hogy a Társaság információfeldolgozó eszközeinek és adatvagyonának biztonsági szintje ne csökkenjen a létrejött partnerkapcsolatok következményeként.

Az alább felsorolt partneri viszonylatokban szerződést a Társaság szerződéskötési szabályzata szerint, a Biztonság szervezeténél történő véleményeztetését követően csak olyan partnerrel szabad kötni, aki / amely tudomásul veszi és vállalja a Társaság szabályzatainak, informatikai biztonsági érdekeinek érvényesítése céljából megfogalmazásra kerülő kívánalmak teljesítését, és lehetőséget biztosít a Társaság számára azok teljesülésének felügyeletére.

a) Ügyfelek

A Társaság ügyfelei különböző módokon kapcsolódnak informatikai rendszereinkhez, pl. passzív adatkérés közérdekű on-line információs rendszerekből (ELVIRA menetrend), általános hozzáférésű on-line szolgáltatás aktív igénybevétele (pl. helyfoglalás, kedvezményes utazásra jogosító kártya vagy igazolvány igénylése).
Ezekben az esetekben a partner vagy ismeretlen, vagy ha ismert, akkor sem kötelezhető speciális intézkedések szigorú betartására, illetve a Társaság biztonsági érdekeinek védelmét célzó eljárások elfogadására. Ezért magukat az ügyfélkapcsolati informatikai rendszereket kell úgy kialakítani, hogy azok használata során a nem szakszerű vagy felelőtlen, esetleg szándékosan rosszindulatú magatartási formák se okozhassanak kárt a Társaságnak, vagy az adott szolgáltatást igénybe vevő más partnereknek.

Az ügyfelek személyes adatainak feldolgozása során az Infotv. által definiált adatkezelés valósul meg. Az adatkezelés törvényes feltételeket is kielégítő végzése érdekében – az informatikai biztonsági szabályok mellett – szigorúan be kell tartani a Társaság Adatvédelmi Szabályzatának előírásait is.

b) Más vasúttársaságok, nemzetközi vasúti szervezetek

A Társaság informatikai rendszerei több szálon is kapcsolódnak vagy kapcsolódhatnak magánvasutakhoz, más nemzeti vagy nemzetközi vasúti szervezet rendszereihez, különösen tájékoztató jellegű adatok cseréje (pl. menetrend), vasútüzemi információk cseréje (forgalmi, igénybevételi adatok, stb.), anyagi-, erkölcsi felelősséget érintő információk cseréje (vasútközi elszámolási adatok, helyfoglalás).

Ezekben a kapcsolatokban – megfelelő szakmai előkészítő tárgyalások után – az érintett feleknek közösen kell megegyezniük a kapcsolatot megvalósító rendszer biztonsági követelményeiben, besorolásában. Az írásba foglalt együttműködési szerződésben, illetőleg annak műszaki vagy más mellékletében külön biztonsági fejezetben kell rögzíteni az informatikai biztonságot érintő hatásköröket, felelősségeket, a biztonság garantálásához alkalmazandó üzemeltetési, felügyeleti és ellenőrzési eljárások részleteit.
Az érintett rendszerek üzleti tulajdonosainak gondoskodniuk kell arról, hogy az együttműködési szerződés és az adott rendszerre vonatkozó RIBSZ biztonsági rendelkezései összhangban álljanak egymással.

c) Informatikai szolgáltatók, beszállítók, szervizek

Ezeknek a kapcsolatoknak az a közös jellemzője, hogy a Társaság (vagy valamely szervezeti egysége) ügyfélként veszi igénybe a partner cég valamely – informatikai biztonságot is érintő – szolgáltatását (Internet kapcsolat, on-line banki szolgáltatás, hardverkarbantartás, javítás, hardver / szoftver bérbeadás, rendszeradminisztráció, vírusvédelem, stb.).

A Társaság biztonsági érdekeit érvényesíteni kell mind a beszállítók megválasztásánál, mind a szerződések megkötésénél a megfelelő biztonsági garanciák beépítésével. Az informatikai beszállítók kijelölése, kiválasztása és a szerződéskötés előkészítése az informatikai vezetőnek a feladata, de a biztonsági megfelelőség megítélésében köteles kikérni és figyelembe venni a biztonsági vezetőnek véleményét a Társaság szerződéskötési szabályzata és jelen szabályzat szerint.

A biztonsági megfelelőség megítélésében figyelembe kell venni a beszállító informatikai biztonsági helyzetét és képességét, informatikai biztonsági megfelelőségét igazoló minősítés meglétét, a (várhatóan) vállalt biztonsági garanciákat.

Egy személlyel, vagy egyszemélyes társasággal nem köthető minősített, illetve a Társaság szempontjából kritikus rendszer kezelésére, illetve üzemeltetésére szerződés. Alap fokozatú rendszerek esetében is kerülni kell az egy-, vagy néhány személyes vállalkozásokkal (pl. bt.), társaságokkal való szerződéskötést, mert az túlzott függőséget jelent a Társaságra nézve, ami magas kockázatot jelent a folyamatos üzemmenetre.

d) Projekt partnerek

A Társaság informatikai rendszereinek korszerűsítésére, új rendszerek létrehozására indított projektek kapcsán az együttműködésre pályázó jelentkezők versenyeztetésénél az informatikai biztonsági előírások maradéktalan érvényesítését is biztosítani kell.

A pályázati felhívásban – a funkcionális követelmények mellett – a pályázóktól elvárt biztonsági követelményeknek is egyértelműen meg kell jelenniük. A pályázati anyagok elbírálása során figyelembe kell venni (lehetőség szerint értékelési súlyarány hozzárendelésével) a pályázó cég informatikai biztonsági felkészültségét, gyakorlatát és képességét, informatikai biztonsági megfelelőségét igazoló minősítés (pl. ISO / IEC 27001) meglétét, a fejlesztésbe bevont munkatársainak oklevéllel bizonyított informatikai (pl. MCSE, MCDBA) és informatikai biztonsági (pl. CISA, CISM) végzettségét, a pályázatnak az informatikai biztonsággal összefüggő fejezeteit, és a vállalt biztonsági garanciákat.

A partnerekkel megkötendő szerződésekben egyértelműen le kell fektetni azokat a kereteket, amelyek szabályozzák a partner számára a Társaság informatikai rendszereinek tárgyiasult elemeihez (infrastruktúra, hardver, adathordozók, dokumentumok) való közvetlen fizikai hozzáférést, a Társaság objektumaiban végzett munkát, szerzői jogi és tulajdonjogi kérdéseket, továbbá a Társaság biztonsági szabályzatainak betartására irányuló kötelezettséget, és azt a jogot, hogy a Társaság utóbbit – akár a partner telephelyén – ellenőrizhesse. A pályázó a Társaságtól a teljesítéshez kapcsolódó biztonsági szabályzatok mellett csak olyan dokumentumot, vagy annak kivonatát kaphatja meg, ami a biztonságot nem érinti hátrányosan.

Informatikai rendszer kialakítását vagy módosítását érintő szerződéseknek kötelező komplex információvédelmi, vagy legalább informatikai biztonsági fejezetet is tartalmazni. Kiemelt projekt munkaszervezetében az információvédelmi szakterület részvételével külön biztonsági alprojektet / projektmodult kell működtetni, aminek feladata a Társaság biztonsági érdekeinek folyamatos érvényesítése.

4.3. Az informatikai vagyon biztonsági besorolása és ellenőrzése

A védelmi intézkedések ezen csoportjának az a célja, hogy mindazok a vagyontárgyak, rendszerelemek, amikből a Társaság informatikai rendszerei felépülnek, egyértelműen azonosíthatók legyenek, naprakész nyilvántartás készüljön róluk, és ki legyen jelölve az értékük megóvásáért felelős személy.

4.3.1. Vagyonleltár

A Társaság informatikai vagyontárgyainak pontos, naprakész leltára az informatikai biztonság menedzselhetőségének alapfeltétele. Erre a célra felhasználhatók a Társaság üzleti folyamatait is kiszolgáló vagyonleltár adatok, amennyiben képesek az informatikai rendszerhez tartozó vagyontárgyak részhalmazának egyértelmű kijelölésére, elhatárolására más típusú vagyontárgyaktól. Az egyes vagyontárgyakat egyéni azonosítóval kell ellátni, és azt fel kell tüntetni az eszközön elhelyezendő címkén. Címkézésére csak olyan technológia használható, amely a tipikus üzemeltetési körülmények (hő, nedvesség, stb.) kedvezőtlen hatásai ellenére is biztosítani tudja hosszabb távon az eszközök azonosíthatóságát. A felügyeleti, ellenőrzési eljárások hatékonyabbá tétele érdekében előnyben kell részesíteni az olyan címkézési technológiákat, melyek mind az emberi-, mind a gépi azonosítás lehetőségét támogatják (pl. vonalkód).

Az egyes rendszerek adatainak értékét (adatvagyonát) az üzleti tulajdonos határozza meg, tartja nyilván és folyamatosan aktualizálja azt. Az érték meghatározásának alapelve, hogy milyen összegbe kerülne a rendszer működőképességének és az abban kezelt adatoknak a helyreállítása a rendszer teljes megsemmisülése esetén.

4.3.2. Információk, informatikai rendszerek biztonsági osztályba sorolása

A Társaság minden informatikai rendszerét a bennük kezelt adatok érzékenysége, az adatokat és a rendszert fenyegető tényezők veszélyessége és azok előfordulási gyakorisága alapján az üzleti tulajdonosnak biztonsági osztályba kell sorolnia, és azt a rendszer jelentős változásakor (pl. ha személyes adatokkal kerül kiegészítésre, vagy ha a vele feldolgozott, üzleti titkot képező adatok minősítési ideje lejárt és ezért az adatot visszaminősítették) felül kell vizsgálnia.

Az informatikai rendszerek besorolását két kategóriában, egyrészt az információvédelem (bizalmasság és sértetlenség együtt), másrészt pedig az adat rendelkezésre állása tekintetében kell elvégezni, és a védelmet mindkét kategóriában a besorolásnak megfelelően kell kialakítani.

Ezek nincsenek egymással semmilyen kapcsolatban, egyik lehet a legmagasabb, a másik ugyanakkor akár a legalacsonyabb fokozatban, és viszont. A rendszer mindkét biztonsági osztályát rögzíteni kell a rendszerterv biztonsági fejezetében vagy az önálló informatikai biztonsági rendszer-tervében, és a rendszer RIBSZ-ében.

Ezt a besorolást minden esetben az adat birtokosa, illetve az adatot feldolgozó rendszer üzleti tulajdonosa hagyja jóvá az ún. kockázatelemzésből nyert információk alapján, annak lezáró aktusaként. Minden további eljárást, fejlesztést, karbantartást, dokumentumot a meghatározott biztonsági osztály követelményeinek megfelelően kell megvalósítani, elkészíteni. A biztonsági osztályba sorolásnak objektív alapokon, az adattal összefüggésben potenciálisan bekövetkező káresemény hatására keletkező kár nagyságától és várható bekövetkezési gyakoriságától függően kell megtörténnie. A káresemények kárérték szerinti besorolásához és a gyakorisági kategóriák értelmezéséhez a 2. sz. mellékletet (Kárérték és kárgyakoriság besorolási táblázata, kockázati mátrix) kell használni az ott leírtak szerint. A potenciális káresemények ilyen minősítése egyúttal az azokat tároló, feldolgozó többi informatikai rendszerelem, illetve a teljes informatikai rendszer biztonsági besorolását is eredményezi.

A minősített (azaz „fokozott” és „kiemelt” osztályba sorolt) informatikai rendszerekben rendre az alacsonyabb osztályok követelményeit, továbbá az adott fokozatra specifikus szabályokat is érvényesíteni kell.

MÁV-csoport szinten használt alkalmazások (pl. GIR, IHIR) saját (a Társaság használatában levő) moduljának besorolási osztályát a többi modultól függetlenül az üzleti tulajdonosnak meg kell határoznia, és az üzemeltetővel (pl. MÁV Szolgáltató Központ Zrt.) kötött szerződésben kell rögzítenie a fokozatnak megfelelő védelmi intézkedéseket.

Számítógépes alkalmazással feldolgozott, üzleti titok kategóriába sorolt adatokat a Társaság üzletititok-védelmi szabályzatának titokköri jegyzékébe is fel kell vetetnie az üzleti tulajdonosnak.

A minősített rendszerekben gondoskodni kell arról, hogy a képernyőn, illetve nyomtatásban megjelenő adatok a biztonsági osztályukra utaló figyelemfelhívó jelzéssel legyenek ellátva. Az ilyen típusú adatokat kezelő, feldolgozó rendszereknél a felhasználói bejelentkezés után a képernyőn fel kell tüntetni a kezelt adatok (azaz a rendszer) minősítését, és fel kell hívni a felhasználó figyelmét azok védelmére. Kivételt képeznek azok a tartalmak, melyek az ügyfelek által hozzáférhető / kezelt rendszerekben kifejezetten az ügyfelek felé irányulnak (pl. az utasok által használt e-Ticket felületeken nem célszerű megjeleníteni a figyelemfelhívó jelzést).

Adathordozók címkéin – ha titokká minősített kategóriába tartozó adatot tartalmaznak – piros színnel, nagybetűvel, jó láthatóan fel kell tüntetni a biztonsági osztályra utaló jelzést a hatályos titokvédelmi törvény, illetve a Társaság Üzletititok-védelmi Szabályzata szerint.

Az adathordozó minősítését és a minősítés felülvizsgálatát azzal megegyező időpontban és ugyanolyan szempontok szerint kell elvégezni, mint azét az informatikai rendszerét, amely(eknek) az adatait tartalmazza.

4.3.3. Alkalmazások biztonsági osztályba sorolásának lépései

a) Az információvédelem (bizalmasság és sértetlenség együtt) szerinti biztonsági fokozat megállapítása

„Alap” biztonsági osztályba kell sorolni az olyan rendszereket, melyek adatainak kompromittálódása sértheti a társaság alapvető funkcióit, különösen az adatok idegen tulajdonába kerülése, de elvesztése, sérülése a társaság részére mérsékelt kockázattal jár.

„Fokozott” biztonsági osztályba kell sorolni:
- az üzleti titkot feldolgozó, kezelő rendszert,
- a személyes adatot feldolgozó, kezelő rendszert (pl. ANDOC, e-Ticket, az IHIR START-os modulja),
- azt a rendszert, amely a Társaság kritikusnak minősülő üzleti folyamatát támogatja (pl. GIR START-os modulja),
- azt a rendszert, amelynek a kockázatelemzése során felvett kockázati mátrixában az elemek több mint 50 %-a legalább a „fokozott” kockázati osztályba tartozik, de a rendszer a „kiemelt” fokozatba nem sorolható be.

„Kiemelt” biztonsági osztályba kell sorolni:
- a különleges személyes adatokat feldolgozó rendszert,
- azt a rendszert, amelynek a kockázatelemzése során felvett kockázati mátrixában az elemek több mint 25 %-a a „kiemelt” kockázati osztályba tartozik.

b) A rendelkezésre állás szerinti biztonsági fokozat megállapítása

1. Meg kell határozni, hogy milyen munkarend szerint kívánják az alkalmazást használni, ezzel megkapjuk az **összesített havi üzemidőt** a következő táblázat alkalmazásával:

a) munkanapokon, munkaidőben:
20 x8,3 = 166 óra / hó
b) munkanapokon, de munkaidőn túl is:
20 x 24 = 480 óra / hó
c) a hét minden napján folyamatosan:
30 x 24 = 720 óra / hó
d) más (konkrétan):
x = óra / hó

2. Meg kell határozni, hogy az így kiszámított havi üzemidőből mennyi az, amikor a rendszernek ténylegesen működnie kell, ezzel megkapjuk a **rendelkezésre állási időt** (pl. folyamatos üzemű a rendszer, és az üzleti tulajdonos döntése szerint a 720 órából 710-et működnie kell, azaz havonként legfeljebb 10 óra kiesés megengedett).

3. Ki kell számolni, hogy a rendelkezésre állási idő hány százaléka az összesített havi üzemidőnek (a példában a 710 óra a 720 órának 98,6 %-a).

4. A következő táblázat adja meg a rendelkezésre állás szerinti biztonsági osztályt.

alap	legalább 95,5 %
fokozott	legalább 99,5 %
kiemelt	legalább 99,95 %

(Példánknál maradva: a biztonsági osztály „alap”, mert nem éri el a „fokozott”-hoz szükséges 99,5 %-ot.)

4.4. Személyi biztonság

4.4.1. Informatikai biztonsági követelmények érvényesítése

Minden felhasználónak ismernie kell az általa használt informatikai eszközök használatának a biztonságát befolyásoló különböző események (biztonsági előírások megsértése, veszélyek, hiányosságok vagy működési zavarok, pl. vírusfertőzés) jelentésének eljárási szabályait. Munkaköri leírásában munkájához számítógép használatára kötelezett munkavállalónak Informatikai biztonsági nyilatkozatot (3. sz. melléklet) kell aláírnia a biztonsági követelmények megismeréséről. A nyilatkozatot a munkavégzés megkezdése előtt alá kell írnia. A munkavállaló által aláírt nyilatkozatot a HR szervezetnél a munkavállaló szolgálati táblájában kell megőrizni.
A munkatársat kiléptető lap (Körözőlap) a munkavállaló kilépési folyamatának részeként azt a célt is szolgálja, hogy a távozó munkavállalónak az általa használt informatikai rendszereket érintő valamennyi jogosultsága garantáltan és dokumentáltan letiltásra kerüljön. Erre vonatkozóan a munkavállaló közvetlen vezetőjének kell intézkednie, és azt a kiléptető lapon aláírásával igazolnia.

4.4.2. A személyiségi jogok védelme az informatikai biztonság megvalósításában

A Társaság a felhasználóknak indokolt esetben biztosít Internet-hozzáférést és e-mail címet. A munkavégzés céljára biztosított számítógépek és az Internet használatának, továbbá az elektronikus levelezés munkáltató általi ellenőrzési, betekintési lehetőségeinek a személyes adatok védelmét érintő általános szabályait a Társaság Adatvédelmi Szabályzata rögzíti. Az ebben meghatározottak szerint a használat szabályairól és a magáncélú használat ellenőrzésének lehetőségéről a munkavállalókat írásban kell tájékoztatni. A tájékoztatásról és a munkavállaló hozzájárulásáról a munkavállaló által aláírt nyilatkozatot a Humán szervezeténél a munkavállaló szolgálati táblájában meg kell őrizni.

4.4.3. Felelősség vizsgálata

Az információvédelmi szakterület a biztonsági eseményeket a lehető legrövidebb idő alatt kivizsgálja. Amennyiben a felelősségre vonás szükségessége fennáll (pl. a munkavállaló vétkes kötelezettségszegésének gyanúja esetén), a biztonsági vezető útján értesíti a munkáltatói jogkör gyakorlóját.
A biztonsággal összefüggő munkavállalói kötelességek megszegésének gyanúja esetén a felelősségi vizsgálat megindítása a munkáltatói jogkört betöltő vezető felelőssége, és egyben kötelessége.

A felelősségi, kártérítési eljárást a Munka Törvénykönyve és a Kollektív Szerződés szerint kell lebonyolítani.

Számítástechnikai rendszer, illetve adatok elleni bűncselekmény (lásd: Btk.) gyanúja esetén a bűncselekmények, szabálysértések elkövetésének észlelése esetén követendő eljárás rendjét szabályozó, hatályos vezérigazgatói utasítás szerint kell eljárni.

A biztonsági események vizsgálatából levont tanulságokat a biztonsági ismeretterjesztésben és az éves biztonsági továbbképzésekben fel kell dolgozni.

4.5. Fizikai és környezeti biztonság

A védelmi intézkedések ezen csoportja a Társaság informatikai rendszereit alkotó tárgyiasult rendszerelemek, illetve azok elhelyezésére szolgáló körletek, telephelyek védelmére, valamint a berendezések folyamatos működéséhez szükséges környezeti feltételek biztosítására szolgál.

4.5.1. Biztonságos elhelyezési körletek kialakítása

A fizikai biztonság megalapozását biztonsági területek kijelölésével kell kezdeni. Minden olyan helyiséget, épületet, telephelyet, amely az informatikai rendszer bármely elemének üzemszerű elhelyezésére vagy tárolására szolgál, be kell sorolni az alábbi szinteknek megfelelően:

a) **kiemelt biztonsági szint:** TÜK iroda, különlegesen fontos számítóközpontok és adathálózati központok, kiemelt biztonsági osztályú alkalmazást futtató szerverek helyiségei,

b) **fokozott biztonsági szint:** számítóközpontok, hálózati rendezők, központi adattárat kezelő, stratégiai, vagy fokozott biztonsági osztályú alkalmazást futtató szerverek elhelyezésére szolgáló szerverszobák, helyiségek,

c) **alap biztonsági szint:** az előző két kategóriába nem sorolt körletek (pl. akár irodában, akár számítóközpontban elhelyezett, alap biztonsági osztályú alkalmazást futtató szerverek helyiségei).

Ezek a szintek a megvalósított (vagy megvalósítandó) biztonsági intézkedések tekintetében jelentenek különbségeket, illetve meghatározzák, hogy milyen biztonsági osztályú eszközök befogadására lehet az adott szintre besorolt területet felhasználni.

4.5.2 Beléptetési intézkedések

A biztonsági területekre az egyes személyek belépését, kilépését – a biztonsági szintnek megfelelően differenciált módon – ellenőrizni, szabályozni kell.

Alap biztonsági szintre besorolt területekre a bejutást – a minimális fizikai védelem kialakítása keretében – az ajtók zárai védik. Ha senki nem tartózkodik a területen, akkor a bejárati ajtókat kulcsra kell zárni. Az adott területen a munkavállalók közvetlen vezetőjének a személyes felelőssége, hogy minden helyiséghez csak az oda önálló belépésre is feljogosított személyek rendelkezzenek kulccsal, és hogy idegen személyek felügyelet nélkül ne tartózkodhassanak a helyiségben. Rendkívüli eseményekre tartalék kulcsokat kell az épületek felügyeleti szerveinél vagy portaszolgálatainál rendszeresíteni – megfelelően biztonságos tárolással –, és eljárásokat kell kialakítani azok felvételének / leadásának dokumentálására, naplózására.

Fokozott és kiemelt biztonsági szintű területeken olyan elektronikus beléptető rendszert kell kiépíteni, amely a vonatkozó MABISZ ajánlásban leírt műszaki követelményeknek megfelel.

A Társaság kulcsfontosságú informatikai eszközeit tartalmazó helyiségek, épületek pontos funkciójára, kialakításának körülményeire vonatkozó információkat **belső adatként**, a nyilvánosság elől rejtve kell kezelni (ne legyenek nyilvános helyen tájékoztató táblák, nyilvános telefonkönyvből, címtárból kiolvasható címek, stb.).

A biztonsági területeket úgy kell kialakítani, hogy azokon belül az információ-feldolgozó tevékenység teljes lefedéséhez szükséges eszközök rendelkezésre álljanak (pl. ne kelljen egy titokká minősített adatot tartalmazó iratot fénymásolás érdekében kivinni a biztonsági területről, mert belül nincs fénymásoló). Ugyanakkor meg kell tiltani a munkafolyamatok szempontjából oda nem illő eszközök, anyagok tárolását, raktározását (pl. a szerverszobákban).

Minden fokozott és kiemelt biztonsági szintű területre az üzleti tulajdonosnak a helyi

sajátosságoknak megfelelő beléptetési utasítást kell kiadnia, amely szabályozza a védett területre munkaidő alatt és azon kívül történő belépés és munkavégzés rendjét mind az állandó munkavállalók, mind az ideiglenes munkavállalók, mind az eseti látogatók vonatkozásában. Ebben az utasításban kell lefektetni: a személyes azonosító eszközök (kártyák, kitűzők, PIN-kódok) használatának, kiadásának, visszavételének, a területre anyagok, eszközök be- és kiszállításának, a területen munkaidőn túli tartózkodásnak, az ideiglenes- és vendég jelleggel belépők nyilvántartásának, kísérésének szabályait.
A beléptetési utasításokat kiadásuk előtt a biztonsági vezetővel véleményeztetni kell, az utasítás csak egyetértésével léphet hatályba.

4.5.3. A berendezések elhelyezése, üzemeltetési környezete

Az informatikai rendszer kulcsfontosságú elemeit (kiszolgáló számítógépek, adathálózati kapcsoló-berendezések, érzékeny adatokat tartalmazó adathordozók, fontos dokumentációk, stb.) a jobb védhetőség érdekében koncentráltan, magasabb biztonsági szintű területek formájában kialakított számítóközpontokban (szerverszobákban, rendezőszekrényekben) kell elhelyezni, működtetni. A berendezések telepítési helyének, elhelyezési körletének megválasztásakor – az adott eszköz rendeltetésétől, biztonsági besorolásától függően – biztosítani kell a zavartalan működéshez szükséges feltételeket:
- biztonságnövelő építészeti megoldások (álpadló, álmennyezet, elektromágneses árnyékoló, illetve tűzgátló külső falak, stb.), bútorzat, világítási rendszer,
- a levegő szükséges hőmérsékletét, páratartalmát, pormentességét biztosító klímaberendezés,
- többutas betáplálással kiépített, redundáns szünetmentes tápáramellátó rendszer, amely vezetett elektromágneses zavaroktól és villámcsapás másodlagos hatásaitól is véd,
- tűz, vízbetörés következtében lehetséges károk mérséklésére szolgáló védelmi rendszerek.

Extrém üzemi környezetben (poros, nyirkos, túl hideg vagy túl meleg helyszíneken) csak olyan berendezést szabad használni, amely – specifikációja szerint – erre kifejezetten alkalmas.
Minden jelentősebb berendezéshez – műszaki specifikációjának előírásai alapján – a fentiek mellett meg kell határozni a megelőző karbantartások rendjét. Ez az adott eszköz üzleti tulajdonosának a feladata, az erre vonatkozó szabályokat a RIBSZ-ben is rögzíteni kell. Ugyancsak a RIBSZ-ben kell rendelkezni az eseti hibajavító karbantartások kezdeményezésének, végrehajtásának szabályairól.

4.5.4. Adathálózat fizikai védelmének szabályai

Az adatkommunikációs kábelek fizikai védelme a nagy (országos méretű) földrajzi kiterjedés, a többnyire folyamatos felügyelet nélküli nyomvonal miatt külön szabályok alkalmazását követeli meg. Cél, hogy az alkalmazott technológiák védjék a kábeleket mechanikai sérülés, elektromágneses zavarok, illegális rácsatlakozás, szándékos rongálás, szabotázs ellen.

Speciális sajátossága a működésnek, hogy az adathálózat elemeit Társaságunk részére a MÁV Zrt. szervezeteinek munkatársai működtetik, biztonságát kialakítják, rendelkezésre állását biztosítják. Társaságunk munkatársainak feladata, hogy az adatátviteli hálózat biztonsága érdekében bevezetett intézkedések, eljárások hatékonyan működjenek. A közvetlen vezetők az irányításuk alatt álló területen ennek érdekében fordítsanak figyelmet a munkaállomások kábelezésének sértetlenségére, a rendezőhelyiségek zártságára, az adathálózat rendelkezésre állására, stb. Nyilvánvaló rendellenességekről tájékoztassák a biztonsági vezetőt, vagy az információbiztonsági koordinátort.

4.5.6. Felhasználói munkaállomások védelme

A felhasználói munkaállomásokhoz bármilyen telekommunikációs eszközt (pl. modem, mobiltelefon) csatlakoztatni a Biztonság kifejezett engedélyével szabad. Az ilyen csatlakozásnak meg kell felelnie a Társaság informatikai biztonsági szabályainak, valamint kizárólag az erre kiképzett és feljogosított személyzet valósíthatja meg. Az engedélyt az érintett közvetlen vezetője írásban (e-mailen) kérje meg a biztonsági vezetőtől.

Minden számítógépes munkaállomáshoz (beleértve tartozékait), továbbá önálló nyilvántartási egységet képező más

informatikai berendezésekhez vagyonleltárban nevesített tulajdonost kell rendelni, akinek feladata, illetve felelőssége:

- a berendezések állagának, épségének megóvása,
- sérülés, hiány azonnali jelentése a közvetlen vezetőnek,
- hordozható eszközök (pl. notebook számítógép, palm-top, projektor) esetén a Társaság objektumain kívül történő használat és a tárolás során a vagyonvédelmi előírások maradéktalan betartása,
- meghibásodásra utaló jelek (szokatlan zajok, melegedés, stb.) esetén a készülék azonnali kikapcsolása, karbantartás igénylése,
- tartós távollét esetére gondoskodás az eszközök más személy általi felügyeletéről, vagy biztonságos helyen történő átmenti tárolásáról.

További védelmi intézkedések

- A berendezések közvetlen közelében tilos minden olyan tevékenység, amely azok sérülését, beszennyezését okozhatja.
- Számítógépek és tartozékaik eltulajdonítása ellen – ahol ezt a közvetlen vezető indokoltnak tartja – mechanikus lopásgátló védelmi eszközökkel, vagy az épület elektronikus riasztórendszerébe kapcsolt tárgyvédelemmel kell a veszélyeztetett berendezéseket ellátni.
- Tilos a számítógépre telepíteni olyan szoftvert, amely valamilyen módon kikerüli a jóváhagyott biztonsági szoftvert vagy ellenőrzéseket.
- A munkaállomásokon 10 perc inaktív működés után automatikusan bekapcsolódó képernyővédelmet kell alkalmazni,
- Ha a számítógép olyan felhasználóhoz kerül, aki nem jogosult a gépen lévő adatok használatára, de egyébként az állományokat máshol használni akarják, akkor kettő példányos mentéssel (CD, DVD), és / vagy szerverre másolással ki kell menteni az adatokat, majd biztonsági törlést kell végrehajtani. Az eszközt csak ezután lehet további használatba adni.
- Amennyiben a számítógépen lévő adatokra a munkavégzéshez a későbbiekben szükség van, de a további felhasználó még nem ismert, a közvetlen vezető intézkedjen az adatok CD/DVD-re történő mentéséről legalább kettő példányban, vagy az informatikai hálózat szerverére történő felhelyezéséről. Nagy mennyiségű adatok esetén technikai megoldást jelent egy új, üres merevlemezre történő mentés elkészítése is. A mentés adathordozóit a közvetlen vezető megfelelő biztonsági intézkedés mellett (zárt szekrény, lemezszekrény, páncélszekrény) köteles tárolni.

4.6. Számítógépes és hálózati szolgáltatások, és az üzemeltetés biztonsági szabályai

4.6.1. Az üzemeltetési eljárások dokumentációja

Az üzemeltetési eljárásokat részletesen dokumentálni kell és a dokumentációt az üzemeltetés helyén hozzáférhetővé kell tenni. A dokumentációinak a munkafolyamat minden részelemére részletes utasításokat kell tartalmaznia. Gondoskodni kell a rendszerdokumentációk biztonságos tárolásáról, és minimálisra kell csökkenteni azok számát, akik hozzáférhetnek.

A biztonsági rendszerek, alrendszerek dokumentációjának tartalmaznia kell a biztonsági funkciók leírását, azok installációját, aktiválását, leállítását és használatát a fejlesztés, valamint az üzemeltetés során. Biztonsági rendszer, alrendszer dokumentációját csak az információvédelmi szakterület munkatársai, illetve az információvédelmi szakterület vezetője által engedélyezett személyek tárolhatják és kezelhetik, az érintett informatikai rendszer biztonsági fokozatának megfelelő módon.

4.6.2. Változásmenedzselés és ellenőrzés az üzemeltetés során

Fokozott és kiemelt biztonsági osztályba sorolt információs rendszer, alkalmazói programok és rendszerleíró paraméterek, rendszerszoftver- és hardver, továbbá hálózati eszközök és rendszerelemek változtatásait ellenőrzött és dokumentált módon kell elvégezni. A változásokat az adott rendszer változáskezelési eljárásrendje alapján ellenőrizni és dokumentálni kell. Ennek során a következő tevékenységeket kell végezni, amelyekben a döntéseket az üzleti tulajdonos hozza:

- változás iránti igény azonosítása, jelentőrendszerbe rögzítése,
- a változások lehetséges hatásainak felmérése,
- döntés a változás megvalósításáról / a változtatási kérelem elutasításáról,
- a változás megvalósításában felelős résztvevők megjelölése,

- a tervezett változások jóváhagyási eljárásainak ellenőrzése,
- a változás kidolgozása,
- a változás tesztelése, nem megfelelőség esetén visszalépés a változás kidolgozása pontra,
- döntés a bevezetésről,
- szükség esetén oktatásuk,
- a rendszer és környezetének archiválása, illetve dokumentálása a bevezetés előtti állapotban,
- a változás bevezetése,
- a tényleges változások dokumentálása,
- a megváltozott környezetről biztonsági mentés készítése.

A változáskezelést az ITIL-ből származtatott fenti lista alapján, társasági szinten egységesen, az erre vonatkozó informatikai szabályok szerint kell kialakítani és működtetni. A teljes változáskezelési folyamatra biztosítani kell az információbiztonsági szakterület biztonsági felügyeletét.

4.6.3. A feladatkörök biztonsági szétválasztása

Az informatikai rendszerek biztonsági beállításához fűződő tevékenységeket a véletlen vagy szándékos visszaélések elkerülése végett szét kell választani úgy, hogy azokat több személynek együttesen (operációs rendszerek, alkalmazások rendszergazdái, informatikai témafelelősei stb.) kelljen végrehajtania. Minősített rendszerek esetében ilyen beállítások csak az információvédelmi szakterület munkatársainak előzetes írásos (pl. e-mail) értesítését követően végezhetők.

A feladatok szétválasztásának szabályai minősített rendszerekben:
- „éles” üzemben működtetett informatikai rendszerben fejlesztések, tesztelések nem folytathatók,
- „éles” adatokkal tesztelést végezni tilos, teszteléshez mindig tesztadatokat kell készíteni (generálni),
- fejlesztés alatt álló rendszerben „éles” üzemi tevékenységet folytatni tilos,
- a fordító, szerkesztő és egyéb segédprogramok „éles” üzemi rendszerben csak abban az esetben legyenek elérhetők, ha ezekre a programokra dokumentáltan és engedélyezetten szükség van,
- a fejlesztők az üzemi rendszerben rendszergazdai (administrator, root, supervisor stb.) jogosultságokat csak kivételesen és ideiglenes jelleggel kaphatnak; amennyiben erre már nincs szükség, a jelszavakat meg kell változtatni, és a rendszer biztonsági beállításait teljes körűen felül kell vizsgálni,
- az információvédelmi szakterület munkatársai részére kiadott rendszeradminisztrátori jogosultságok, csak a biztonsági tevékenységgel kapcsolatos munkák során, naplózottan használhatók.

A biztonsági ellenőrzést a végrehajtó szervezettől és a menedzsmenttől függetlenül, az információvédelmi szakterület hatáskörében kell működtetni. Részei: a rendszergazdák tevékenységének monitorozása, az eseménynaplók elemzése és a funkcionális felügyelet.

4.6.4. Védelem rosszindulatú programok ellen

A programok és az adatfeldolgozó kapacitások ki vannak téve a rosszindulatú programok (számítógépes vírus, féreg, „trójai faló”, keylogger, logikai bomba, stb.) bejutása veszélyének. A felhasználóknak ismerniük kell a rosszindulatú és engedély nélküli programok alkalmazásával járó veszélyeket.

A rosszindulatú programokkal szembeni védekezést szűréssel, megfelelő teszteljárások kidolgozásával, a programok és adatok használatba vétele előtti ellenőrzésével, továbbá az adminisztrátori jogosultsággal végzett tevékenységek korlátozásával kell megvalósítani. A rosszindulatú programok elleni védekezés részét képezi a felhasználók tájékoztatása és oktatása, a hozzáférés-védelem, továbbá a változtatások felügyelete és ellenőrzése is.

A Társaság vírusvédelmi rendszerét és annak üzemeltetését az informatikai stratégia és az informatikai biztonsági stratégia előírásai szerint elkészített RIBSZ alapján kell kialakítani. Ebben tervezni kell a vírusvédelmi szoftverek kiválasztásának elveit, beszerzésének gyakoriságát, a szükséges liszensz-számot, a rendszeres frissítés módját és felelőseit, továbbá ki kell jelölni a rendszer kialakításának és fenntartásának felelőseit.

Éves szolgáltatási szerződésben gondoskodni kell mind a Társaság számítógépes hálózatára kapcsolódó, mind pedig az önálló (stand alone) PC-k és a hordozható számítógépek

vírusvédelméről. A frissítési eljárást a szerver és hálózati munkaállomás részen is automatikussá kell tenni. A kiszolgáló rendszereken és a kliens gépeken központosított menedzsmentű, automatikus napi frissítésű vírusmintával rendelkező, különböző gyártótól származó vírusvédelmi eszközöket kell alkalmazni.

A vírusok és rosszindulatú programok támadása által jelentkező kár csökkentése érdekében a PC-k operációs rendszerei vonatkozásában központosított, automatikus biztonsági javítócsomag (patch) menedzsmentet kell alkalmazni.

Az összes érintett munkavállalóra kiterjedő felhasználói oktatásnak ki kell térni a vírusvédelmi rendszerre vonatkozó ismeretekre is.

Hordozható számítógép esetén a felhasználó kötelessége a vírusvédelmi rendszer minél gyakoribb automatikus frissítéséről gondoskodni oly módon, hogy számítógépét VPN útján, vagy közvetlenül a belső hálózatra csatlakoztatja.

4.6.5. Az adatmentések

A munkaállomásokon készített saját állományokat a szervereken központilag kialakított saját könyvtárakban kell tárolni. Ez biztosítja az állományok folyamatos rendelkezésre állását, mivel a szervereken tárolt adatok rendszeresen mentésre kerülnek.

Hordozható számítógép (hordozható PC, tablet, stb.) esetében a keletkezett dokumentumokat vagy engedélyezett fájlokat a szerverre kell felmásolni az előző bekezdésben meghatározott könyvtárba. Bármely eszköz meghibásodása, elvesztése, ellopása esetén, ha az adatállományok a központi szerverről nem reprodukálhatóak, akkor minden felelősség az eszközt használó munkatársat terheli.

Biztonsági másolatokat kell készíteni az informatikai alkalmazások által kezelt adatokról, amelyek felhasználásával az éles adatállomány szükség esetén reprodukálható. A visszaállításra való alkalmasságot évente legalább egy alkalommal ellenőrizni és a teszt eredményét dokumentálni kell. Emellett:

- a rendszerek RIBSZ-ében a megtervezett mentési és visszaállítási eljárásokra üzemeltetési előírásokat kell készíteni, és azok betartását rendszeresen ellenőrizni kell,
- a biztonsági mentéseket földrajzilag külön telephelyen, és az adott biztonsági osztályra előírt követelményeknek megfelelő külön helyiségben kell tárolni (ennek részleteit RIBSZ-ben kell meghatározni),
- a mentések nyilvántartását a RIBSZ előírásainak megfelelően kell vezetni, naprakészségét az üzleti tulajdonosnak rendszeresen ellenőriznie kell,
- az időszakos, archiválandó (pl. éves) adat- és rendszer-mentéseket a jogszabályokban meghatározott ideig, de legalább a mindenkori számviteli törvény előírásai szerinti megőrzési időig bármikor visszakereshetően, helyreállíthatóan kell tárolni és hozzáférhetővé tenni.

4.6.6. Operátori, rendszergazdai tevékenységek naplózása

Az informatikai rendszer üzemeltetése során operátori (rendszergazdai) naplót kell vezetni az üzemeltetési eseményekről, amit az üzleti tulajdonosnak rendszeresen ellenőriznie kell.

Az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert kell kialakítani, hogy annak segítségével utólag megállapíthatóak legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Egyúttal lehessen ellenőrizni a hozzáférések jogosultságát, meg lehessen állapítani a felelősséget, valamint az illetéktelen hozzáférés megtörténtét vagy annak kísérletét. A minimálisan regisztrálandó események a következők:

- rendszerindítások, -leállások, leállítások,
- üzemzavarok, rendszerhibák és korrekciós intézkedések,
- programindítások és -leállások, leállítások,
- a rendszer erőforrásaihoz hozzáférési jog kezelése,
- az adatállományok és kimeneti adatok kezelésének visszaigazolása,
- a rendszer biztonságát érintő műveletek (felhatalmazott személyeké is).

A további naplózandó eseményeket (pl. az azonosítási és hitelesítési mechanizmus használata) rendszerfüggően kell meghatározni és a RIBSZ-ben tételesen rögzíteni kell.

4.6.7. Adathordozók és infokommunikációs tartalmú dokumentumok biztonságos kezelése és szállítása

Az eszközök károsodásának megelőzése, és az üzleti tevékenységekben okozott fennakadás megakadályozása érdekében gondoskodni kell az adathordozók ellenőrzéséről és fizikai védelméről. Meg kell előzni a dokumentumok, a számítástechnikai adathordozók (szalagok, lemezek, kazetták, memóriakártyák, stb.), az input / output adatok és a rendszerdokumentációk károsodását, eltulajdonítását és engedély nélküli törlését. Minden adathordozót újraalkalmazás előtt, továbbá felszabadítás és selejtezés után az adatok biztonságos megsemmisítését eredményező megfelelő eljárással törölni kell. Az adathordozók eredeti felhasználási helyéről történő elvitelére, illetve a meghibásodott adathordozók cseréjére csak az adott szervezeti egység vezetője adhat engedélyt.

Biztosítani kell, hogy az adathordozók kezelése – a vonatkozó iratkezelési szabályok szellemében – a tartalmazott adatok szempontjából egyenértékű papír dokumentumokkal azonos biztonságot eredményező módon történjék. Az adattípus (minősítés) felismerhető jelölését a számítástechnikai berendezéssel előállított adattároló és megjelenítő eszközökön biztosítani kell (lásd: 4.3.2. pont).

Adathordozók meghibásodása esetén – ha azon más módon pótolhatatlan (vagy saját erőből csak nagyon magas költséggel pótolható) adatok voltak – külső szakértőket kell megbízni az adatok visszanyerésével. Titokká minősített adatok esetén kiegészítő intézkedéseket kell tenni az adatok visszaállítása alatti illetéktelen megismerésének, felhasználásának megakadályozására (pl. titoktartási kötelezettség előírása).

Sérült adathordozók garanciális cseréje esetén – ha a meghibásodott eszköz titokká minősített adatokat is tartalmazott – az eredeti alkatrészt nem, vagy csak az adatok kiolvasását lehetetlenné tevő hatástalanítást követően, a Biztonság közreműködésével szabad a karbantartó részére átadni.

Az adathordozók tárolására vonatkozó fizikai védelem követelményeivel kapcsolatban a rendszer minősítéséhez igazodva, annak RIBSZ-ében meg kell határozni:

- a rendszerhez használt / használható tárolók környezeti paramétereire vonatkozó előírásokat, és a paraméterek normál értékeinek biztosítására, ellenőrzésére vonatkozó intézkedéseket,
- az elöregedésből fakadó adatvesztés elleni megelőző intézkedéseket (pl. rendszeres átírás),
- az adathordozók másodpéldányainak biztonságos tárolására vonatkozó előírásokat,
- a rendszer- és a felhasználói szoftver törzspéldányok biztonságos tárolására, valamint a használati másodpéldányok készítésére vonatkozó előírásokat.

Az információ a fizikai szállítás során történő átvitel esetén ki van téve az illetéktelen hozzáférés és visszaélés veszélyének. A számítástechnikai adathordozók biztonságos szállítása ezért az alábbi szabályok alkalmazásával történhet:

- szállítás során átadás-átvételi bizonylat szükséges,
- fokozott vagy kiemelt biztonsági osztályba sorolt adatot tartalmazó adathordozót csak megfelelően felcímkézett, lezárt csomagolásban szabad szállítani,
- épületen kívüli szállítás esetén a legrövidebb és leggyorsabb útvonalat kell kiválasztani,
- fokozott vagy kiemelt biztonsági osztályba sorolt adatot tartalmazó adathordozót tömegközlekedési eszközön szállítani tilos,
- épületen kívüli szállítás esetén – MABISZ ajánlást figyelembe véve – megfelelő tárolóeszköz szükséges,
- mágneses adathordozó (mágneslemez, merevlemez) szállításkor és használatakor elkerülendő a nyilvánvalóan erős mágneses tér (pl. nagyfeszültségű távvezetékek, a képcsöves PC monitor és a hangfalak közelsége, stb.),
- mágneses adathordozó szállításakor szükség szerint gondoskodni kell az árnyékolásról,
- szállítás során a vagyonbiztonság érdekében fokozott figyelemmel kell eljárni,
- az adathordozót tilos őrizetlenül hagyni (pl. a gépkocsiban),
- az adathordozókat óvni kell a fizikai sérülésektől.

Rendkívüli esemény (pl. az adathordozó elvesztése, a rajta levő adatok sérülése vagy megsemmisülése) esetén a szervezeti egység

(a szállítást elrendelő) vezetőjét – szükség esetén a rendőrséget is – értesíteni kell. A vezetőnek haladéktalanul meg kell tennie a további károk elkerülése érdekében a szükséges lépéseket, valamint ezzel egy időben tájékoztatnia kell az információvédelmi koordinátort az eseményről és a megtett intézkedésről (távbeszélő, fax, e-mail).

Minősített adatot tartalmazó adathordozó tartalmát a Biztonság közreműködésével selejtezést és megsemmisítést megelőzően visszaállíthatatlanul törölni kell. Ha ez nem lehetséges, az adathordozót meg kell semmisíteni.

A biztonságra már nem veszélyes, törölt adathordozó selejtezését és megsemmisítését a vonatkozó informatikai előírások szerint, a Biztonság felügyeletével, dokumentáltan kell végezni. A selejtezett eszközökről bármilyen alkatrészt, hulladékdarabot felhasználni bármilyen célra tilos.

Semmilyen esetben, még átmenetileg sem másolható titokká minősített adat külső (csatlakoztatott) adattárolóra. De a nem minősített üzleti jellegű adatok másolása esetében is a külső eszközt használaton kívül biztonságosan el kell zárni, vagy más módon védeni kell illetéktelen hozzáférés ellen.

Amennyiben már nincs szükség az anyagok külső eszközön való tárolására, azokat haladéktalanul és visszaállíthatatlan módon törölni kell onnan.

A külső tárolón tárolt adatok biztonsági mentéséről is a felhasználónak kell gondoskodnia, ha az szükséges.

A rendszerek teljes életciklusában gondoskodni kell a rendszert érintő dokumentumok megfelelő kezeléséről. A rendszer életciklusa alatt alapvetően a következő dokumentumok keletkezhetnek és változhatnak:

- projektalapító dokumentum,
- projektértékelő és projekttag értékelő dokumentumok,
- projektzáró beszámoló,
- értekezletek emlékeztetői,
- logikai rendszerterv és biztonsági rendszerterv,
- teszt forgatókönyv,
- tesztelési jegyzőkönyv,
- telepítési jegyzőkönyv,
- telepítés és konfigurációs kézikönyv,
- konfigurációs jegyzőkönyvek (APN, tűzfal, router, felhasználói szoftver operációs rendszer stb.),
- átadás-átvételi jegyzőkönyvek, teljesítés-igazolások,
- éles üzembe helyezés átadás jegyzőkönyv,
- Rendszerszintű Informatikai Biztonsági Szabályzat,
- Felhasználói / Üzemeltetői dokumentáció, kézikönyv,
- oktatási dokumentáció, tematika, oktatási segédlet,
- Informatikai Működésfolytonossági Terv,
- Változáskezelési Eljárásrend.

Amennyiben egy rendszer életciklusában egyéb dokumentumok is keletkeznek, akkor ugyanezek a szabályok érvényesek a tárolásukra és kezelésükre.

Valamennyi dokumentumot az üzleti tulajdonosnak kell tárolnia a rendszer minősítésének megfelelő biztonsággal. Ha rendszer bármely szempontból is fokozott, vagy kiemelt minősítést kapott, akkor a dokumentációkat legalább lemezszekrényben kell tárolni. Az üzleti tulajdonosnak gondoskodnia kell arról, hogy a dokumentumokhoz csak a szükséges minimális körben férjenek hozzá a munkatársak.
Az Üzleti tulajdonos feladata, hogy a rendszer életciklusában folyamatosan kövesse, követtesse a változásokat, és azokat a dokumentumokban is érvényesítse. A dokumentumok elektronikus elérése esetén az üzleti tulajdonos határozza meg, milyen jogosultsági feltételekkel lehet azokat elérni a központi szerveren.

4.6.8. Adatcsere, adattovábbítás

A Társaság más szervezettel kizárólag a Biztonság által véleményezett és engedélyezett írásbeli szerződés alapján bonyolíthat informatikai eszközökön adatcserét. A szerződésben rendelkezni kell az érzékeny adatok kezelésére is. Az adatcsere biztonsági feltételeire vonatkozó megállapodásokban meg kell határozni:

- az adatfeladás, az adatátvitel és az adatátvétel ellenőrzésének és bejelentésének eljárási szabályait,
- az adatok biztonságos átvitele előkészítésének és tényleges átvitelének műszaki szabványait,

- az adatvesztéssel kapcsolatos kötelezettséget és felelősséget,
- az adatátvitel során a biztonságos (szükség esetén rejtjelezett) környezet előírásait minden érintett félnél,
- az érzékeny adatok védelméhez szükséges speciális eszközök igénybevételét (pl. kriptográfiai eszközök, virtuális LAN),
- a hitelesség, letagadhatatlanság kritériumait (pl. elektronikus aláírás).

A Társaság más külső társaságok részére folytat adatküldést. Adatküldést csak a Biztonság által arra feljogosított személyek folytathatnak. A beállításokat a Biztonság engedélye alapján az informatikai szolgáltató végzi. A kapcsolat engedélyezése előtt a kommunikációs portokat és a kommunikációra kijelölt eszközöket meg kell határozni. Az adattovábbítást minden esetben titkosított átviteli eljárással kell megvalósítani
Érzékeny adatok informatikai hálózaton történő továbbítása kizárólag titkosított adattovábbítással, csak a kommunikációban résztvevő felek kölcsönös azonosítása és hitelesítése után kezdeményezhető. Érzékeny adatok továbbítása esetében a küldést megelőzően legalább 512 bites kulccsal titkosítani kell. Aszimmetrikus titkosítási megoldás választása esetén (pl. PGP) a titkosító-kulcsot a partner generálja és juttatja el a publikus részét, illetve a hitelességet ellenőrző kulcs ujjlenyomatot a Társaságunk részére. A kulcs megújításért a partner feleljen. Egy kulcs egy évnél tovább nem használható. Erről a pályázati kiírásban, a szerződés tervezetében gondoskodni kell.

4.6.9. Az elektronikus kereskedelem biztonsága

A korszerű piaci igények kielégítésére szolgáló elektronikus szolgáltatások (pl. menetjegy-értékesítés, IC helyfoglalás) biztonsága komplex védelmet igényel, mert az adatkezelés során adatcserére, személyes adatok kezelésére és nyilvános hálózat (Internet) igénybevételére egyaránt sor kerülhet.

A hatékony védelem megvalósítása érdekében vállalkozói szerződésben garantált, integrált biztonságot kell az ilyen rendszer kifejlesztése során kialakítani, melynek legfontosabb elemei:

- a vállalkozó kötelezése a Társaság információvédelmi szabályzatainak betartására,
- a hozzáférés szabályozása és ellenőrzése,
- egységes azonosítás és hitelesítés kialakítása,
- elektronikus aláírások alkalmazása, rejtjelezés, kulcsmenedzsment (PKI),
- a behatolási kísérletek figyelése,
- biztonsági naplózás a hozzáférések, az azonosítás és a hitelesítés ellenőrzéséhez,
- az auditálhatóság biztosítása.

4.6.10. Az elektronikus levelezés biztonsága

Az elektronikus levelezés biztonságát több veszély fenyegeti. Ilyen lehet pl. az üzenetek illetéktelen elérésének vagy módosításának, illetve a szolgáltatás megtagadásának a veszélye, emberi hibákból eredő veszélyeztető tényezők, pl. rossz címzés vagy irányítás, titokká minősített adatok véletlen továbbításának lehetősége, a feladó- és címzett-hitelesítési problémák, illetve a levél átvételének bizonyítása, a kívülről hozzáférhető címjegyzékek tartalmával való visszaélési lehetőségek, vagy pedig a távolról bejelentkező felhasználó biztonsági problémái. A felsorolt kockázatok csökkentése érdekében a következőben felsorolt biztonsági szabályokat kell betartani.

- Az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelméről folyamatosan gondoskodni kell (pl. nyomon kell követni a szoftverfrissítések, service pack-ok és security-patch állományok megjelenését).
- Az elektronikus levelező rendszeren keresztül történő támadások esetén, amennyiben a rendszer védelme átmenetileg nem biztosított, – pl. olyan vírustámadás esetében, amikor a vírusvédelmi rendszerek még nem nyújtanak kellő védelmet – az Interneten keresztül bonyolított elektronikus levélforgalmat ideiglenesen le kell állítani.
- Az elektronikus levelezés forgalmát az üzleti titkok és a belső adatok kiszivárgásának elkerülése érdekében tartalmilag szűrni kell.
- Magáncélú levelezésre a munkahelyi e-mail cím nem használható. Ilyen üzenetek küldése / továbbítása a munkahelyi e-mail címről tilos mind a Társaságon belüli, mind azon kívüli címekre (pl. Gmail, Freemail, Citromail, Vipmail, Iwiw, Skype,).

- Amennyiben a levelező partner magáncélú üzenetet küld a munkahelyi e-mail címre, akkor a partnert meg kell kérni, hogy a munkahelyi levelezésre biztosított címre továbbiakban ne küldjön magáncélú leveleket.
- File-megosztó, video-letöltő Internetes címek látogatása, média-állományok (pl. mp3) letöltése kizárólag a munkával összefüggésben, a közvetlen vezető kezdeményezésére, a Biztonság engedélyével, az Informatika egyidejű tájékoztatása mellett engedélyezett.
- Minden felhasználót oktatni kell arról, hogy az általa a munka céljára kapott eszközökkel készített, a Társaság levelező rendszerében tárolt és továbbított levelek a Társaság tulajdonát képezik, ezért a Biztonság ezekhez az állományokhoz a vizsgálathoz szükséges mértékig betekintési joga van. Az ellenőrzés során biztosítani kell az ellenőrzött jelenlétét és magánszférájának a sértetlenségét. A betekintés további szabályait a Társaság Adatvédelmi Szabályzata tartalmazza.
- A Társaság levelező rendszere a Társaság üzletmenetétől idegen (pl. nem utazási lehetőségekről vagy utazási kedvezményekről szóló reklám), valamint egyéb üzleti célokra nem használható.
- A Társaság elektronikus levelezési címjegyzéke külső szervezetnek a Társaság belső adatvédelmi felelőse engedélyével, törvényben meghatározott esetekben szolgáltatható ki.
- A társaság munkavállalóinak alapértelmezésként rendelkezésre álló postafiókméretet, a csatolható melléklet méretét, az egyszerre megadható címezettek számát az informatikai lehetőségek függvényében kell kijelölni.
- A levelekhez tilos rövid filmeket, hangfájlokat (wma, wmw, mp3, stb. kiterjesztésű állományok) csatolni. Ettől eltérő szabályokat indokolt esetben a Biztonság engedélyez.
- A közvetlen vezető és az érintett munkatárs egyaránt felelős azért, hogy a munkatárs munkaviszonyában történő változás esetében postafiókjának állapota, rendelkezésre állása megfelelően legyen kezelve.
- A Társaság minden informatikai eszközzel (számítógéppel) rendelkező munkatársa részére postafiókot biztosít. A postafiók méretét az informatikai vezető határozza meg. A küldendő és beérkezett mellékletek együttes méretét – a technikai lehetőségek függvényében – korlátozni kell. A korlát eseti túllépésére a küldőnek be kell szereznie a Biztonság engedélyét.
- Hivatali célú Társaságon belüli levelezés csak a Társaság által biztosított postafiókokban lehetséges. Tilos hivatali célú leveleket külső általános célú, vagy közösségi célú postafiókokba küldeni. Hivatalos levél csak abban az esetben küldhető általános célú postafiókba, ha a Társasághoz ilyen postafiókról érkezett megkeresés (pl. önéletrajz küldése, közérdekű adat kérése), vagy a hivatalos partner szerződésben a kapcsolattartásra ilyen postafiókot adott meg.
- A Társaság által biztosított postafiókot a felhasználónak kell karbantartania. Amennyiben a karbantartást nem tudja elvégezni, köteles az Informatika támogatását kérni. A postafiók helytelen kezeléséből, beteléséből eredő károkért a felhasználó a felelős.
- A Társaság levelező rendszerében csoportokat lehet létrehozni, hogy ne kelljen adott esetben egyenként név szerint címezni. Egy felhasználó több csoportba is tartozhat. A csoportok létrehozását és karbantartását mindig egy illetékes vezetőnek kell kezdeményeznie, illetve végeznie. A csoportok felülvizsgálatát az Informatika végzi évente legalább egy alkalommal. Az ellenőrzés eredményéről írásban tájékoztatást ad a Biztonság információvédelmi szakterülete részére.
- A Társaság a levelező rendszerében a Társaságon kívüli személyek, szervezetek részére nem biztosít levelezési lehetőséget, postafiókot és e-mail címet.
- A Társaság a munkavállalói érdekképviseletek részére a velük kötött megállapodás szerint biztosít hozzáférési lehetőséget, postafiókot és e-mail címet.

Fenti szabályok mellett a Felhasználók biztonsági kötelezettségei című (1. sz.) melléklet 15. pontja további részleteket tartalmaz az elektronikus levelezés biztonságát illetően.

4.6.11. VPN alkalmazása

A Társaság a hordozható informatikai eszközökhöz (lap-top, palm-top stb) az informatikai szolgáltatón keresztül VPN hozzáférést biztosít. A VPN kapcsolaton keresztül a felhasználó ugyanazt a munkahelyi környezetet éri el, mint az asztali eszközéről (levelezés, központi szerver, programok stb.).

Ilyen eszközökről VPN használata nélkül tilos a Társaság informatikai rendszerébe belépni. A VPN felhasználásra a következő szabályok vonatkoznak:

- A Társaságtól kapott eszközzel (pl. lap-top) munkát végző vezetők, továbbá azon munkatársak részére, akik a vonatkozó szabályzatba foglaltak szerint távmunkát végeznek, kötelező a VPN használata.
- Magántulajdonú eszközre VPN eljárást tilos telepíteni.
- A telepített VPN eljárásokról az Informatika köteles nyilvántartást vezetni.
- A telepített VPN kapcsolaton keresztül biztosítani kell az operációs rendszer mindennemű frissítéseinek és a vírusvédelmi rendszer folyamatos frissítéseinek felhasználó független végrehajtását.
- Kiemelt biztonsági osztályú rendszerhez távolról csatlakozni tilos.
- Tilos üzleti titkot távolról elérni, és kezelni, a hordozható eszközre letölteni.
- A távolról csatlakozó gépek esetében, a kliens gépre telepített VPN kapcsolat használatával azonos időben más WiFi és/vagy VPN és/vagy Internetes csatlakozás tilos. Az Internet elérésének is a VPN kapcsolton keresztül kell történnie.
- A VPN jogosultság visszavonását a munkatárs közvetlen vezetőjének kell kezdeményeznie, vezetők esetében az informatikai vezető is jogosult erre.
- Külföldről csak a Társaság által biztosított mobil Internet, GSM kapcsolat és VPN együttes használatával lehet a Társaság informatikai rendszerébe belépni.

4.6.12. QR-kód alkalmazása

A QR-kódok alkalmazása biztonsági kockázatokat rejt magában. A QR-kódokban elhelyezett un. URL címek kártékony, rosszindulatú kódot tartalmazó helyekre mutathatnak. A QR-kódok használata során előfordulhat a nyomtatott kód felülragasztása, felülírása, elektronikus továbbítása esetén a lecserélése, módosítása. Ezek megelőzése, kiküszöbölése érdekében a QR-kódok használatakor kötelező a biztonsági előírások betartása. A rendszer hamisítás elleni védelme a QR kód tartalmának elektronikus aláírásával biztosítható, míg az adatok illetéktelen személy általi megismerése ellen azok titkosításával lehet védekezni.

Az informatikai rendszereinkben alkalmazott QR-kódok előállítása során titkosítást és tömörítést kell alkalmazni és a kódot elektronikus aláírással kell ellátni. Az utasok, ügyfelek tájékoztatására szolgáló QR-kódok előállítása során a fentiek nem alkalmazhatók, ekkor a partnert tájékoztatni kell a QR-kód leolvasás kockázataira.

Az informatikai rendszereinkben használt QR-kódok leolvasása alkalmával a QR kódban lévő adatok (kódok) automatikus futtatását technikai eljárásokkal kell megakadályozni.

Annak érdekében, hogy a készülékre, illetve a Társaság hálózatába káros kódok ne kerülhessenek be, a kód olvasására alkalmazott eszközökről a kódolvasási folyamat során a Társaság belső hálózatán kívülre tilos bármilyen kommunikációt kezdeményezni. Ezt technikai eljárásokkal kell megakadályozni.

Tilos a hivatalos levelezés aláírását saját létrehozású QR kóddal helyettesíteni, vagy kiegészíteni.

4.7. Hozzáférés-menedzsment

A Társaság a munkatársak munkaköri feladatának megfelelő szervezeti, fizikai és logikai intézkedések alkalmazásával korlátozza az adatokhoz, a számítástechnikai rendszerekhez és a hálózatokhoz való hozzáférést, az alábbiak szerint.

4.7.1 A hozzáférés-menedzsment általános szabályai

A hozzáférési jogosultságok megállapításának alapját az érintett munkavállaló tevékenységi és munkaköri leírásában rögzített szerepköre, külsős beszállítók és karbantartók alkalmazottai esetében a vonatkozó szerződésben leírt feladat ellátásához szükséges és indokolt adathozzáférési igény képezi. Ennek során érvényesíteni kell azt a – biztonságpolitikában lefektetett – követelményt, hogy a munkavállaló és külsős csak a munkájához feltétlenül szükséges adatokhoz és csak a szükséges időtartamban férhessen hozzá. Fokozott védelemben kell részesíteni a minősített (pl. üzleti titkot képező adatokat feldolgozó, vagy személyes adatokat kezelő, feldolgozó) informatikai rendszereket.

A Társaság informatikai rendszeréhez való hozzáférés kizárólag AD (Active Directory) felhasználásával történhet.

Külső fél minden esetben a Biztonság engedélyével kerülhet felvételre az AD rendszerbe. Az AD kezelését a mindenkori informatikai szolgáltató végzi, és a Biztonság felügyeli.

Az egyes alkalmazások biztonsági feltételeit úgy kell kialakítani, hogy a hozzáférési jogosultságok érvényesítése, az adatkezelés eseményeinek nyomon követhetősége és személyi felelősséghez köthetősége garantálható legyen. A hozzáférési jogosultságokra vonatkozó elképzelést már a rendszer tervezésének időszakában, a biztonsági osztálynak megfelelő követelményszinten ki kell alakítani. Az informatikai rendszerrel dolgozó minden munkatárs a védelmi rendszertervben konkrétan meghatározott szerepkörbe sorolandó, és megkapja a szerepkörre meghatározott hozzáférési jogokat. A munkaköröktől történő eltérést a tervezés során a projekt vezetőjének, az üzemeltetés során pedig az üzleti tulajdonosnak kell meghatározni és az információbiztonsági koordinátorral egyeztetni.

Akinek a munkaviszonya megszűnt, az a rendszer szolgáltatásait nem veheti igénybe, és erőforrásait nem használhatja. A Társaság munkavállalóinak felhasználói azonosítóját munkaviszonyuk megszűnésével, a külső munkavállalók felhasználói azonosítóját megbízatásuk lejártával, illetve munkavégzésük befejezésekor haladéktalanul le kell tiltani. Ennek biztosításáért a munkavállaló közvetlen vezetője, illetőleg a megbízást adó és a munkavégzést irányító személy a felelős.

A munkaviszonyukat huzamosabb ideig szüneteltető (pl. gyermek szülése), illetve 30 napon túlmenően távollevő (pl. külföldi kiküldetés, elhúzódó gyógykezelés) munkatársak felhasználói azonosítóját AD szinten, valamint a postafiókját a levelező rendszerben fel kell függeszteni. Ennek biztosításáért a munkavállaló közvetlen vezetője felelős. A letiltásra úgy kell intézkednie, hogy az már a távollét első napján hatályos legyen.

A munkavállalók áthelyezése kapcsán felmerülő jogosultsági változásokat (megszűnő felhasználói azonosítók letiltása, vagy a jogosultságok törlése, illetve új azonosítók vagy jogosultságok létrehozása) az áthelyezéssel egy időben, haladéktalanul át kell vezetni. Ennek kezdeményezése az áthelyezés előtti és az áthelyezés utáni közvetlen vezető feladata.

Ha munkavállaló munkája során bármely ok miatt már nem használ számítógépet, akkor közvetlen vezetőjének azonnal intézkednie kell a jogosultságai visszavonásáról, és ha volt, postafiókjának kezeléséről, megszüntetéséről.

A felhasználó beosztottal rendelkező közvetlen vezető a közvetlen irányítása alá tartozó munkavállaló munkaviszonyának bármilyen okból való megváltozásakor a munkavállaló által az informatikai rendszerekben (pl. DMS-Poszeidon) kezelt adatokhoz, dokumentumokhoz történő további hozzáférésről gondoskodni köteles.

Amennyiben a munkavállaló kilépésekor, vagy munkakörének megváltozásakor a munkakört átvevő személy kiléte még nem ismert és az informatikai eszköz más személy részére kiadásra kerül, akkor az adatok mentéséről és az eszközről történő letörléséről gondoskodni kell. A mentést 2 példányban CD/DVD lemezre kell elkészíteni, vagy az informatikai hálózat szerverére kell felhelyezni. Nagy mennyiségű adatok esetén technikai megoldást jelent egy új, üres merevlemezre történő mentés elkészítése is. A mentés adathordozóit a közvetlen vezető megfelelő biztonsági intézkedés mellett (zárt szekrény, lemezszekrény, páncélszekrény) tárolja.

A jogosultságokban bekövetkezett változásokat mindig az adott rendszer Rendszerszintű Informatikai Biztonsági Szabályzatának megfelelően kell végrehajtani. Mérlegelni kell, hogy áthelyezés esetén milyen jogosultságok maradhatnak meg a munkavállalónál.

A felsővezetők esetében a hozzáférési jogosultságok módosításában, visszavonásában a biztonsági vezető közreműködését kell kérni.

Azokban a rendszerekben, amelyek regisztrálják a felhasználó utolsó bejelentkezésének időpontját, továbbá az Active Directory-ban ha egy felhasználó azonosító 30 napot meghaladóan inaktívnak bizonyul (azaz a felhasználó a rendszer szolgáltatásait ez idő alatt egyszer sem vette igénybe, illetve nem lép be a Társaság hálózatába), azonosítóját le kell tiltani, és erről a munkavállaló közvetlen vezetőjét értesíteni kell, megjelölve az érvénytelenítés okát.

A felhasználó-azonosítónak minden esetben egyedinek kell lennie, (azaz semmilyen körülmények között sem adható ki különböző

felhasználók részére megegyező azonosító). A felhasználói azonosítók és jogosultságok rendszerében bekövetkezett mindennemű változást (az ellenőrizhetőség érdekében) minden rendszerben külön-külön naplózni kell.

Az adott felhasználói rendszerhez kiadott rendszergazdai, rendszeradminisztrátori azonosítókat és jelszavakat lezárt, lepecsételt borítékban, biztonsági zárral zárható fa vagy lemezszekrényben kell tárolni. A lezárt borítékot a lezárónak alá kell írni, a lezárás dátumának feltüntetésével. A borítékokat az üzleti tulajdonosnál, vagy az általa kijelölt vezetőnél kell tárolni úgy, hogy azok rendkívüli esetben hozzáférhetőek legyenek.

Felhasználók csak a biztonsági vezető külön írásos engedélyével rendelkezhetnek a munkaállomáson rendszeradminisztrátori jogosultsággal. A jogosultságot a Biztonság információbiztonság területénél nyilván kell tartani.

Az informatikai rendszerekben biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága a szerepkörüknek megfelelő legyen. Ennek érdekében:

- a jogosultságokat az üzleti tulajdonosnak rendszeres időközönként ellenőriznie kell; az általános felhasználók esetében ezt évente, a fokozott biztonsági besorolású rendszerekben félévente, míg a kiemelt besorolásúban 3 havonta kell megtenni,
- a szerepkörök változásakor a hozzáférési jogosultságokat felül kell vizsgálni és az új szerepkörnek megfelelően módosítani kell.

A munkaállomásokon távoli hibaelhárítást végző szolgáltató esetenként a felhasználó nevében végez műveleteket a számítógépen a jelentkező hiba megismerése, javítása céljából. Ennek során biztosítani kell, hogy a munkaállomás feletti felügyeletet kizárólag a felhasználó beleegyezésével vehesse át, továbbá a felhasználó azonosítójával végzett tevékenységét naplózni kell a felelősség elhatárolása érdekében. Amennyiben a hibaelhárítást végző hívta telefonon a felhasználót és így kezdeményezte a számítógép távoli átvételét, akkor a hibaelhárítást végző visszahívásával ellenőrizni kell, hogy valóban a megbízott Help Desk szolgálat munkatársáról van szó. A felhasználónak a képernyőn figyelnie kell a nevében, az általa kezelt adatokkal végzett műveleteket és szükség esetén közbe kell avatkoznia.

A Társaság részére informatikai vagy infokommunikációs fejlesztést végző külső társaság munkavállalója kifejezetten a rendszer fejlesztéséhez szükséges fejlesztői (DV) és tesztelői környezethet (TE) kaphat időszakos hozzáférést. A hozzáférés igényét minden esetben az üzleti tulajdonos kezdeményezi a Biztonság szervezeténél, amit az engedélyez vagy elutasít. Az igénylésben meg kell határozni a felhasználó nevét, a rendszer nevét és a környezeteket, a jogosultsági szintet, és az időtartamot. Az alap bejelentkezés kizárólag az AD útján történhet. Rendszerszinten az üzleti tulajdonosnak kell a jogosultság megadását és visszavonását kezdeményezni. Ha a külső felhasználó távoli hozzáférést igényel, azt VPN kapcsolattal kell megvalósítani. A VPN kapcsolat kialakításáról és visszavonásáról az üzleti tulajdonosnak kell rendelkeznie.

4.7.2. A felhasználói jelszó kezelése

Az informatikai rendszerekben a felhasználók hitelesítésének alapvető módja a jelszó megadása. A felhasználói jelszavak kezelésére a következőekben, továbbá az 1. sz. melléklet 4. pontjában felsorolt szabályok a mérvadók.

- Végleges használatra kapott jelszó átadása csak biztonságos csatornán történhet, a felhasználó előzetes – pl. személyes – azonosítása után.
- A kezdeti jelszó kivételével jelszavakat vagy a jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani tilos.
- Az első bejelentkezés alkalmával a kapott ideiglenes jelszót kötelező lecserélni.
- Saját jelszavát az előírt periódus szerint minden felhasználó köteles megváltoztatni, azon belül a jelszópolitikához illeszkedően tetszés szerinti időpontban cserélheti.
- A jelszavakat – a biztonsági másolat kivételével – nem szabad felírni, papíron tárolni. Amennyiben ez elkerülhetetlen (pl. a kezdeti jelszó), akkor gondoskodni kell a jelszónak a közvetlen vezetőnél, zárt borítékban történő, biztonságos tárolásáról, átadásáról
- Automatikus bejelentkezési eljárások (pl. batch fájlok, vagy funkcióbillentyűhöz rendelt makrók) nem tartalmazhatnak felhasználói jelszót.

- A hálózati informatikai rendszerbe (AD, Active Directory) történő bejelentkezéskor az alábbi jelszópolitika az érvényes:

- a rendszer az utolsó 3 jelszóig emlékszik a jelszavakra, azaz azokat nem lehet újra használni,
- 42 naponként jelszót kell változatni,
- 5 nap után megváltoztatható a jelszó,
- legalább 8 karakteres jelszót kell használni,
- a jelszó összetételében az alábbi 4 csoport közül legalább három csoport elemeiből, minimum egy karaktert kell, hogy tartalmazzon:
  - kisbetű (a-z)
  - nagybetű (A-Z)
  - szám (0-9) és
  - különleges karakterek (! @ # $ % ^ & * ( ) _ +| ~ - = \ ` { } [ ] : " ; ' < > ? , . /)
- a jelszó sem kis, sem nagy ékezetes betűt nem tartalmazhat
- 5 sikertelen bejelentkezési kísérlet után a felhasználói fiók zárolódik,
- ha sikertelen bejelentkezések miatt zárolódik a felhasználói fiók, 10 perc múltán a tiltás feloldódik,
- 10 perc múlva a rendszer nullázza a sikertelen bejelentkezések számlálót,

A hálózati bejelentkezési jelszópolitikára meghatározott fenti paraméterek kielégítik az „alap” biztonsági osztály követelményeit.

Elfelejtett jelszó esetén a következő szabályok érvényesek:

1. A felhasználó köteles közölni közvetlen vezetőjével, hogy a jelszavát elfelejtette.
2. A közvetlen vezető e-mailben értesíti az informatikai szolgáltatót, hogy pontosan melyik felhasználó, melyik gépén történt az esemény.
3. Az informatikai szolgáltató elvégzi az új jelszó generálását, és azt SMS-ben, ha az nem lehetséges, akkor telefonon szóban köteles közölni a közvetlen vezetővel.
4. A közvetlen vezető szóban elmondja a megküldött jelszót a munkatársnak, aki köteles ezzel bejelentkezni és a bejelentkezés során azt kikényszerítve megváltoztatni, figyelembe véve az általános szabályokat.
5. Amennyiben a közvetlen vezető SMS-ben kapta meg a jelszót, akkor köteles a kapott SMS-t az eszközéről törölni.

4.7.3. A jelszó használata az informatikai alkalmazásokban

- A felhasználói jelszó szerkezeti szabályaival (bonyolultság) szemben támasztott követelményeket (lásd: 4.7.2. pont) minden esetben a rendszer informatikai biztonsági osztálya határozza meg.
- A jelszó házirendet rendszerfüggően, az egyes RIBSZ-ekben kell rögzíteni.
- Az informatikai rendszerekben a jelszó a képernyőn nem jeleníthető meg. A jelszó bevitelénél biztosítani szükséges, hogy a billentyűleütésekor egy eltakaró karakter (pl. *) megjelenjen.
- Minősített rendszerekben a felhasználó hitelesítésére erős authentikációt kell alkalmazni (pl. ún. erős jelszó, chip-kártya).
- A felhasználói jelszavakkal kapcsolatban (amennyiben az adott rendszerben erre lehetőség van) már a fejlesztéskor szabályozni kell a minimális jelszóhosszat, a jelszó-történet tárolását, a központi jelszómegadás utáni első bejelentkezéskor a jelszó kötelező cseréjét, a jelszó maximális élettartamát, a jelszó minimális élettartamát, a jelszó zárolásának szabályait, a jelszóképzési szabályokat.
- A számítógépes rendszerekben a jelszavakat tilos nyílt formában tárolni. Ha a rendszer ilyen védelmet automatikusan nem nyújt, akkor a jelszófájlokat külön védelemmel kell ellátni.
- Minősített rendszerekben a felhasználónak új jelszava átvételét ellenőrizhető úton (pl. e-mail), vagy személyesen minden esetben vissza kell igazolnia.
- Az információvédelem szempontjából alap biztonsági osztályba sorolt rendszerek elérésekor, amennyiben az informatikai eszközbe történő belépés címtár (AD) alapján valósul meg, akkor a felhasználó azonosítása történhet a számítógépbe beléptetett felhasználói azonosító alapján, automatikusan a címtárból, újabb felhasználói azonosítás nélkül.
- A minősített informatikai rendszerekben a felhasználói azonosításra használt jelszó nem egyezhet meg a felhasználó AD belépését biztosító jelszóval!

4.7.4. Hordozható eszközök használata, távoli hozzáférés

4.7.4.1. Hordozható számítógép használata

A hordozható informatikai eszközön (társaság által biztosított laptop) illetve otthoni saját PC-ről, távoli hozzáféréssel végzett távmunka esetén is meg kell teremteni ugyanazokat az informatikai biztonság feltételeket, amelyek kialakításra kerültek a Társaság munka-állomásainak védelmére. Az eszközt csak akkor lehet a felhasználó részére átadni, ha az előbbi feltételeket a Biztonság megvizsgálta és maradéktalanul megfeleltnek értékeli. A Társaság adatátviteli hálózatára kapcsolódás kizárólagosan megengedett módjai hordozható számítógép használata esetén:

a) a védett munkahelyi környezetből közvet-lenül, vagy ún. dokkoló állomáson keresztül csatlakozva (a hagyományos munkaállo-máséval megegyező módon),
b) a védett munkahelyi környezetből vezeték nélküli hálózat (WiFi) útján a 4.7.5. pont szerint,
c) nem védett környezetből (pl. otthonról vezetékes hálózatról, vagy nem a Társaság által biztosított GSM kommunikációs szolgáltatással), távoli hozzáféréssel, a Társaság által biztosított védett VPN (Virtual Private Network) adatátviteli csatornán.

Sem védett, sem nem védett környezetből más módon, pl. az OWA (Outlook Web Access), vagy OAW (Outlook AnyWhere) szolgáltatás használatával tilos csatlakozni a Társaság informatikai rendszeréhez!

A Társaság informatikai rendszeréhez a fentiektől (a)-c) bekezdések) eltérő technológián alapuló kapcsolódás tilos!

A hordozható számítógépekkel végzett tevékenység szabályai:

- az informatikai szolgáltatóval vizsgáltatni kell, hogy a hálózatra csatlakozni kívánó számítógép állapota biztonsági szempontból megfelelő-e (van-e rajta aktulizált vírusirtó, megfelelő biztonsági patch-ekkel ellátott operációs rendszer fut-e rajta, stb.),
- a hordozható eszközt használók hozzá-férését azonosításhoz és hitelesítéshez kell kötni; hitelesítésre erős authentikációt kell alkalmazni (pl. erős jelszó, chip-kártya),
- a hordozható számítógépeken az IBSZ által meghatározott vírusvédelmi és biztonsági eszközöknek aktív állapotban kell lenniük; a felhasználó ideiglenesen sem iktathatja ki a védelmet,
- a hordozható eszközökön belső adatot, üzleti titkot képező adatot tilos tárolni, továbbá személyes adatot pedig csak védetten, rejtjelezve szabad,
- a hordozható eszközök lopás elleni védelmére fokozott figyelmet kell fordítani, felügyelet nélkül hagyni csak olyan helyen szabad, ahol az általános vagyonvédelmi szabályok teljesülnek (pl. felügyelet nélküli gépkocsiban nem, még a csomagtartóban sem).
- hordozható számítógépre csak felhasználói jogosultság adható. Ennek megváltoztatására csak igénylés alapján a Biztonság adhat engedélyt. A megváltozott jogosultságot minden esetben az informatikai szolgáltató köteles beállítani.

A távoli hozzáférés biztonsági szabályai:

- kiemelt biztonsági osztályú rendszerhez távolról csatlakozni tilos,
- fokozott biztonsági osztályú rendszerben végzendő munkához védett (rejtjelezett) csa-tornáról kell gondoskodni, a kommunikációt titkosítani kell olyan algoritmussal (legalább 512 bites titkosítás), ami jelentősen megne-hezíti a tartalom visszafejtését,
- fokozott biztonsági osztályú rendszerben végzendő távmunkát a munkavállaló közvetlen vezetőjének kezdeményezésére, az adott rend-szer üzleti tulajdonosának jóváhagyásával, írásban engedélyezi a biztonsági vezető. Az engedély másolatát megküldi az informatikai vezetőnek, aki intézkedik a szükséges módo-sítások, beállítások, telepítések elvégzésére. Az engedélyben rögzíteni kell:

- azon rendszer(ek) megnevezését, ame-ly(ek)re az engedély kiterjed,
- a hivatali helyiségeken kívüli munkavégzés engedélyezési időszakát,
- a munkavégzéshez az alkalmazott részére (otthonában) a Társaság által biztosított berendezések azonosítását, ill. a szükséges berendezések és anyagok átadási és elszámolási módját,

4.7.4.2. PDA, okostelefon használata

PDA, okostelefon informatikai alkalmazásban való használata esetén alapelv, hogy csak a célnak megfelelően konfigurált eszközt lehet alkalmazni. A készülék konfigurációit (pl. funkciók tiltása) a Biztonság szervezetével előzetesen egyeztetett informatikai biztonsági szabályok szerint kell meghatározni. A Társaság informatikai rendszerének szervereivel folytatott kommunikációnak minden esetben titkosítottnak kell lennie, legalább 512 bites titkosítással. Az eszközön tárolt adatokat szintén titkosítani kell. PDA-hoz, okostelefonhoz és egyéb eszközhöz kiegészítő elemeket (pl. memóriakártya) a Biztonság szervezetének engedélye alapján és az előzetesen egyeztetett informatikai szabályok szerint lehet csatlakoztatni. A hordozható eszközökkel az alábbi szabályok betartása mellett végezhető munka.

– Az eszközre telepített alkalmazást csak az előzetesen meghatározott informatikai biztonsági osztály követelményei szerinti felhasználó név és jelszó azonosítással lehet használni. A hitelesítési eljárást központi szerver támogatásával kell elvégezni. Az eszközt úgy kell konfigurálni, hogy arra felhasználó csak a hivatalos alkalmazásboltokból származó szoftvert tudjon telepíteni. Minden telepítést követően vírusellenőrzést kell végezni az eszközön.
– Minden eszköznek rendelkeznie kell olyan folyamatosan frissülő vírusvédelmi eljárással, ami a társaság egyéb eszközeihez igazodik, a hordozható eszközön futó alkalmazásokat nem befolyásolja és viszont.
– Minden eszközön olyan egységes beállítást kell alkalmazni, ami lehetővé teszi az operációs rendszer folyamatos frissítését.
– A kizárólag szolgálati célra kiadott (pl. jegyvizsgálói okostelefon) PDA, okostelefon stb. eszközt, melyen olyan alkalmazás fut, ami központi szerver kommunikációt igényel kötelezően a mobilszolgáltató által APN-be kell szervezni, és az APN kapcsolat csak a Társaság szervere felé történő kommunikációt engedélyezze.
– A hordozható eszközök használatát központi, átfogó felügyeleti rendszerrel kell támogatni.
– Az egyéni használatra kapott hordozható (PDA, okostelefon, stb.) készüléket a szükséges és elégséges jogosultság megadásával kell a felhasználó részére konfigurálni.

4.7.4.3. Jegykiadó automaták használata

A jegykiadó automaták belső számítógépe egy mobil kapcsolattal ellátott eszköz, ami APN-be szervezett hívásokkal kommunikál a központi szerverrel. Amennyiben vezetékes kapcsolat nem építhető ki, akkor az APN-be szervezés kötelező. Az adattovábbításnak minden esetben titkosítottnak kell lennie, mivel a rendszer érzékeny adatokat is forgalmaz. A jegykiadó automaták belső számítógépének operációs rendszerét, vírusvédelmét folyamatosan frissíteni kell. A jegykiadó automatákat önálló felügyeleti rendszerbe kell vonni. Felügyeleti rendszeren kívüli jegykiadó automatát tilos üzemeltetni.

4.7.5. Vezeték nélküli (WLAN, WiFi) hálózat használata

A vezeték nélküli hálózatok egyedi beállításait az alábbiak figyelembe vételével a hálózat RIBSZ-ében kell meghatározni.

WiFi hálózat használatának az alábbi feltételei vannak:

- a központi szintű beállításokat a központi irodaépületben (Budapest, Könyves Kálmán krt.) a MÁV Zrt. IT szakterülete az épület informatikai üzemeltetője útján biztosítja,
- a központi irodaépületen kívüli WiFi hálózat használata tilos,
- a felhasználónak rendelkeznie kell a Biztonság írásbeli engedélyével a használatra, amit közvetlen vezetője útján kell igényelnie,
- a Társaság vezetékes hálózatához történő csatlakozáskor a vezeték nélküli kapcsolatot ki kell kapcsolni,
- a Társaság Internet elérését vezeték nélküli hálózaton tovább megosztani tilos,
- vezeték nélküli eszköz használatba vétele, telepítése a biztonsági vezető írásos engedélye nélkül tilos,
- a vezeték nélküli hálózatokhoz a hozzáférést szabályozni és naplózni kell,
- ilyen hálózat kialakítása előtt annak biztonságát tervezni, majd a beállításokat ellenőrizni kell,

- megfelelő titkosítást kell alkalmazni (legalább WPA2-AES 256) (WEP és WPA használata tilos!),
- hitelesítést kell alkalmazni (pl. 802.1x EAP-PEAP, token),
- tűzfalat kell alkalmazni,
- behatolás megelőző rendszert (IPS) kell alkalmazni,
- hálózat hozzáférés-szabályozási rendszert kell alkalmazni,
- a beléptetés előtt ellenőrizni kell az eszközök biztonsági állapotát (pl. Microsoft NAP, azaz Network Access Protection, vagy Cisco Systems NAC, azaz Network Admission Control).

Kliens szintű beállítások, feltételek:

- a felhasználó gépében lennie kell a WiFi kommunikációra alkalmas hardver eszköznek,
- a WiFi titkosítási megoldásai közül legalább a WPA2 szintű védelmet biztosító eljárás használata engedélyezett (WEP és WPA használata tilos!),
- vezeték nélküli kommunikáció beállításánál csak meghatározott (SSID-vel azonosított) hálózatba való belépés engedélyezett, az alapértelmezett hálózatnak a Társaság hálózatának kell lennie,
- a vezeték nélküli kommunikációra alkalmas eszközökben a munkavégzésen kívül a kommunikációs eszközt, interfészt ki kell kapcsolni.

4.7.6 Távmunka

A Társaság munkavállalói részére a távmunka a mindenkori hatályos távmunka végzési szabályzat szerint engedélyezett. Az informatikai biztonsági feltételek az otthon végzett munkával kapcsolatosan a következők:

- saját eszközön tilos távmunkát végezni, csak a Társaság által biztosított számítógépen, eszközökön megengedett,
- a számítógépet az informatikai szolgáltató által felkészített módon kell átadni, úgy, hogy
- azon működjön az operációs rendszer és a vírusvédelmi rendszer frissítése, valamint csak
- olyan szoftver lehet telepítve, ami feltétlenül szükséges a feladatok végrehajtásához,
- felhasználó rendszergazdai jogosultságot nem kaphat,
- bejelentkezése a Társaság informatikai rendszerébe csak VPN felhasználásával történhet,
- amennyiben routert is használ, azt az informatikai szolgáltatónak kell megfelelően konfigurálni és a beállításokat dokumentálni,
- A Társaság Biztonság szervezete jogosult a számítógép beállításait annak kiszállítása előtt, majd annak használatát és a környezetét előre egyeztetett időpontban biztonsági szempontból ellenőrizni.

4.8. Informatikai rendszerek fejlesztésének biztonsági szabályai

Új rendszer fejlesztésében - továbbá meglevőnek a módosításában értelemszerűen - az alábbi szabályoknak kell teljesülni.

4.8.1. Döntés a rendszer kialakításáról

A döntés pillanatától kezdve a rendszerbe be kell építeni az informatikai biztonság elemeit. Olyan rendszer nem alakítható ki, amelyik rontaná az informatikai biztonság meglevő állapotát és színvonalát. Minden felhasználói informatikai rendszernek együtt kell működnie a társaságnál használt vírusvédelmi rendszerrel, egymást kölcsönösen működésükben nem zavarhatják.

Minősített kategóriájú új informatikai rendszer, vagy a meglevő ilyen rendszereket érintő bármilyen módosítás csak ellenőrzött módon vezethető be, vagyis szabályszerű jóváhagyási, probléma- és változáskezelési eljárások alkalmazásával. Az ilyen rendszerek esetében fel kell készülni a rendszer esetleges meghibásodása esetén követendő, a működési folytonosságot fenntartó eljárások alkalmazására.

4.8.2. A rendszerfejlesztés előkészítése

Az előkészítés lépéseit az Informatikai fejlesztés biztonsági feladatai és dokumentumai c. táblázatban (4. sz. melléklet a) része: Projektindítás) összefoglaltak szerint kell elvégezni. A táblázatot a nem projektszerűen végrehajtott és kisebb fejlesztésekben értelemszerű egyszerűsítésekkel kell alkalmazni. A felsorolt feladatok végrehajtója a projektvezető, illetve, ha ilyen még nincs kijelölve, vagy a fejlesztés nem projektszerűen folyik, akkor a fejlesztést kezdeményező szervezeti egység vezetője.

Az előkészítésnek fontos lépése az üzleti tulajdonos kijelölése. Ez a 4.2.2. a) pont alapján az informatikai vezető felelőssége. A rendszer biztonságát az üzleti tulajdonos a saját igényei és lehetőségei szerint valósítja meg, mert döntési kompetenciával ő rendelkezik a szükséges erőforrások mozgósításához.

A fejlesztésre vonatkozó **pályázati kiírásban** szerepeltetni kell a biztonságra vonatkozó alapkövetelményként a Társaság információvédelmi szabályzatainak betartására irányuló pályázói kötelezettséget.

Az **Ajánlatkérési dokumentumban** meg kell adni a kezelendő adatok érzékenységét, ha van, akkor a minősítését, a rendszer információvédelem és rendelkezésre állás szempontjából történő besorolását, a védelmi igényt és célokat, a jogszabályokból és egyéb társasági belső utasításokból fakadó biztonsági kötelezettségeket. Szerepeltetni kell, hogy az ajánlat biztonsági szempontból csak akkor elfogadható, ha:

- a kitűzött védelmi célokra megfelelő szinten reagáló fejezetet (részeket) tartalmaz,
- az ajánlattevő nyilatkozik, hogy csak jogtiszta szoftvert, illetve rendszert szállít,
- nyilatkozik arról, hogy elfogadja a Társaságnál érvényes biztonsági szabályokat a rendszer kialakításában.

Előnyben kell részesíteni azt a pályázót, aki / amely rendelkezik informatikai vagy informatikai biztonsági színvonalát bizonyító minősítéssel (MSZ ISO/IEC 15408, MSZ ISO/IEC 27001, stb. szerint).

A fejlesztésre vonatkozó **szerződésnek** külön fejezetben kell foglalkoznia az informatikai biztonsággal. Ebben a fejezetben szerepeltetni kell a szállítandó szoftver, illetve termék:

- teljesítendő informatikai biztonsági követelményeket,
- biztonsági tanúsításával, minősítésével kapcsolatos feltételeket,
- dokumentációjának biztosításával kapcsolatos követelményeket,
- használati (futtatható) illetve forráskód felhasználásának és ellenőrzési jogának, a licencek felhasználásának a feltételeit,
- szavatosságával, jótállásával, auditálhatóságával kapcsolatos feltételeket,
- garanciális időn túlmenő szervizelési feltételeit, úgymint rendelkezésre állási idő, reakció-idő, tartalék alkatrész biztosítása, cserefeltételek, tartalék eszközök,
- titoktartási (ha a rendszer titokká minősített adatokat is kezel), és adatvédelmi (ha a rendszer személyes adatokat is kezel) követelményeket, megállapodásokat,
- a szállító nyilatkozatát, hogy a védelmi rendszer tervezéséhez és megvalósításához használt információkat és dokumentumokat átadják,
- a szállító nyilatkozatát, hogy az informatikai rendszer fejlesztése során eleget tesznek a Társaság valamennyi biztonsági szabályzatának.

A pályázat kiírásába és értékelésébe, továbbá a szerződés szövegének kialakításába minden esetben be kell vonni a Biztonság információbiztonsági szakterületét, aminek a hatásköre kizárólag az informatikai biztonsági megfelelőség biztosítására, a Társaságnál fennálló szintjének megőrzésére terjed ki. A Szerződéskötési Szabályzat értelmében a szerződést akkor lehet megkötni, ha azon a „biztonsági szignó” is szerepel.

A **Rendszerkoncepció**, vagy a **Projekt alapító okirat** c. fejlesztési dokumentumban meg kell határozni az alapvető informatikai biztonsági követelményeket. A rendszer biztonságával kapcsolatosan meg kell határozni a szereplőket, meg kell nevezni a biztonsági határokat, adatátviteli hálózat biztonsági feltételeit, az életciklus kezelési feltételeit.

4.8.3. A rendszer biztonsági kockázatainak felmérése

A fejlesztendő rendszer megvalósítása során az informatikai biztonságot a rendszerbe integrálva kell kialakítani, amihez ismerni kell a rendszert konkrétan fenyegető veszélyeket, ismerni kell a várható biztonsági kockázatokat. Az ehhez szükséges lépéseket az Informatikai fejlesztés biztonsági feladatai és dokumentumai c. táblázatban (4. sz. melléklet b) része: Kockázatelemzés) összefoglaltak szerint kell elvégezni. A táblázatot a nem projektszerűen végrehajtott és a kisebb fejlesztésekben értelemszerű egyszerűsítésekkel kell alkalmazni.

Az ott felsorolt feladatokat az üzleti tulajdonos irányítja és a rendszerre vonatkozó biztonsági igényei alapján a beszállítóval végezteti a megvalósítási szerződés keretében.

A kockázatelemzés szakaszban részletesen fel kell tárni a rendszert fenyegető tényezőket. Ehhez csoportosítani kell a vizsgálandó szempontokat a:

- környezeti infrastruktúra,
- hardver eszközök,
- adathordozók,
- dokumentumok,
- szoftver,
- adatok,
- kommunikáció,
- szolgáltatások,
- személyi elemcsoportok vonatkozásban.

Ezekhez a csoportokhoz kell egyedenként meghatározni a fenyegető tényezőket a Kockázatelemzés lépései c. táblázat szerint (5. sz. melléklet). A későbbiekben valamennyi védelmi intézkedést ezek tükrében, a ténylegesen fennálló informatikai biztonsági kockázatok ellen fellépve kell megtenni.

4.8.4. A rendszer biztonságának tervezése

A kockázatelemzést végző által tett javaslat alapján a rendszert az üzleti tulajdonosnak biztonsági osztályba kell sorolnia a 4.3.2. pont szerint. Ezt követően intézkedéseket kell tennie az azonosított kockázatok kezelésére és meg kell határoznia a maradó (nem kezelt) kockázatokat.

A következő fázisban a RIBSZ-et megalapozó Informatikai Biztonsági Rendszertervet (vázlata: 6. sz. melléklet), kisebb rendszerekben a Rendszertervben informatikai biztonsági fejezetet kell kialakítani. Az ehhez szükséges lépéseket az Informatikai fejlesztés biztonsági feladatai és dokumentumai c. táblázatban (4. sz. melléklet c) része: A rendszer biztonságának tervezése) összefoglaltak szerint kell elvégezni. A fejezetben, illetve önálló dokumentumban röviden fel kell sorolni azokat a tervezési kiindulási alapokat, amelyek az adott rendszerre specifikusak, és részletes kidolgozást igényelnek, azaz meg kell adni az ezekre a témakörökre részletes feladatokat, szabályokat előíró RIBSZ vázlatát. Tartalmának szigorú összhangban kell lennie a korábbi fázisban meghatározott biztonsági osztályra vonatkozó informatikai biztonsági követelményekkel, és az üzleti tulajdonos ezen felüli biztonság és más igényeivel.

A rendszer védelmét fizikai, logikai és adminisztratív területen kell megvalósítani. Ezek részleteit jelen szabályzat, a minősített biztonsági osztályokra a szabályzat több helye és a 7. sz. melléklete tartalmazza.

A rendszer tervezése során az informatikai biztonsági osztály meghatározása következményeként adott, hogy kell-e titkosított adatáramlást, elektronikus aláírást és az ezekhez kapcsolódó tevékenységeket ellátni. Az Informatikai Biztonsági Rendszertervben (Rendszerterv informatikai biztonsági fejezetében) tervezni kell az ide vonatkozó védelmi intézkedéseket is. A RIBSZ-ben kell részletesen kifejteni az Informatikai Biztonsági Rendszertervben (Rendszerterv informatikai biztonsági fejezetében) felsoroltakat. Meg kell adni az ott vázolt, tervezett funkciók, eljárások, védelmi intézkedések, stb. konkrét megvalósítási módszerét, felelősét, paramétereit. A 12. sz. melléklet tartalmazza a RIBSZ általános vázlatát, amit azonban szűkíteni lehet, ha a tervezési alapokmányban – az Informatikai Biztonsági Rendszertervben (Rendszerterv informatikai biztonsági fejezetében) – foglaltak szerint az adott tartalmi elemre nincs szükség.

Felhasználói adatbázisok, továbbá a rendszerszoftverek és az operációs rendszer által generált adatbázisok (pl. naplófájl) védelmét úgy kell biztosítani, hogy felhasználó azokat közvetlenül ne tudja elérni, abban ne tudjon közvetlenül műveleteket végezni. A közvetlen és nem naplózott elérést és módosítást az üzemeltető és a rendszergazda részére is tiltani kell.

Adatbáziskezelő rendszer naplózási tevékenységét úgy kell konfigurálni, hogy csak a szükséges naplózási funkciók legyenek aktivizálva. Szükség esetén az üzleti tulajdonos döntése, vagy informatikai szempontok alapján a napló adatállományok térbeli (méret) és időbeni határát korlátozni kell.

Információvédelmi szempontból fokozott vagy kiemelt biztonsági osztályba sorolt rendszerek teljes adatbázisát, vagy egyes – a minősítés alapjául szolgáló adatokat konkrétan tartalmazó – moduljait, részeit titkosítottan kell tárolni. A tikosító kulcsnak legalább 512 bitesnek kell lennie. A kulcskezelés védelmére külön intézkedéseket kell tervezni és megvalósítani a rendszerben.

A rendszer fejlesztése során a fejlesztő társaságnak több környezetet kell kialakítania a feladata végrehajtása során. Az alábbi leírástól a Biztonság előzetes engedélyével szabad eltérni.

a) Fejlesztői környezet (DV): kifejezetten a fejlesztők részére létrehozott környezet melyben a fejlesztés, és a fejlesztői belső tesztek történnek.
b) Teszt környezet (TE): kifejezetten a megrendelő részére kialakított környezet, melyben megrendelő felhasználói a teszteket végzik. Ennek a környezetnek hasonlónak kell lennie, mint az éles környezet. Ebben a környezetben fejlesztői tevékenység végzése tilos!
c) Minőségbiztosítási környezet (QA): kifejezetten a megrendelő részére kialakított környezet, melyben a megrendelő felhasználói teljes körű tesztet végeznek. Felépítésében minden tekintetben azonosnak kell lennie az éles környezettel. Ebben a környezetben fejlesztői tevékenység végzése tilos!
d) Oktatási környezet (ED): kifejezetten csak oktatás céljára használható környezet. Felépítésében és adattartalmában minden tekintetben azonosnak kell lennie a QA környezettel. Ebben a környezetben fejlesztő tevékenység végzése tilos!
e) Éles környezet: kifejezetten a rendszer üzemeltetésére szolgáló környezet. Ebben a környezetben fejlesztői tevékenység végzése tilos!

Az egyes környezetek közötti átjárás szabályai a következők.

- Fejlesztői környezetből teszt környezetbe csak akkor megengedett szoftvert és adatokat másolni, ha fejlesztő kijelentette, hogy a fejlesztést befejezte, és az üzleti tulajdonos engedélyezte a másolást, telepítést.

- Teszt környezetből minőségbiztosítási környezetbe csak akkor megengedett szoftvert és adatokat másolni, telepíteni, ha a felhasználói alaptesztelések sikeresen befejeződtek, és ezt a tesztelők jelezték az üzleti tulajdonosnak. A másolás, illetve telepítés végrehajtását az üzleti tulajdonos írásban engedélyezi.

- Minőségbiztosítási környezetből éles környezetbe csak akkor megengedett szoftvert másolni, vagy telepíteni, ha a minőségbiztosítási környezetben a tesztek teljes körűen sikeresen végrehajtódtak.

- Minőségbiztosítási környezetből oktatási környezetbe csak akkor megengedett szoftvert másolni, vagy telepíteni, ha a minőségbiztosítási környezetben a tesztek teljes körűen sikeresen végrehajtódtak.

További általános szabályok:
- A szoftver telepítését, másolását és adatbázisok telepítését másolását minden esetben kizárólagosan az informatikai szolgáltató végezheti a fejlesztőtől kapott utasításoknak megfelelően.
- Ha TE és QA környezetekben hiba történt, akkor minden esetben a fejlesztői környezetben kell a változtatásokat végrehajtani és ismételten meg kell kezdeni a teszteléseket.
- A Biztonság engedélyezhet a rendszer sajátosságainak figyelembevételével olyan tesztelési eljárást, ahol nem aktuális, de lényegében éles adatokkal történhet a tesztelés.
- Minden környezetben történt változást dokumentálni kell megjelölve az okokat és a következményeket. A dokumentumokat az üzleti tulajdonosnak, vagy megbízottjának kell átadni, és jóváhagyatni.

Minden rendszert alkalmazásbiztonság tekintetében is tesztelni kell. A tesztelést a QA környezetben kell végrehajtani. Ellenőrizni kell, hogy az alkalmazás – különösen dobozos termék esetén – nem tartalmaz-e veszélyes kódot, vagy végez-e olyan műveleteket, mellyel adatokat továbbít nem megfelelő helyekre, vagy nem megfelelő helyekről adatokat, eljárásokat hív be. Amennyiben ilyen jellegű eljárásra csak gyanú is felmerül, az eljárás további tesztelését, bárminemű fejlesztését kötelezően le kell állítani, és független szakértő bevonásával meg kell kezdeni az alkalmazás teljes felülvizsgálatát. A vizsgálat költségeit a fejlesztőnek/beszállítónak kell viselnie.

4.8.5. A rendszer használatba vétele

A rendszerben megvalósuló valamennyi elemet a rendszer használatba vételét megelőzően biztonsági megfelelőség szempontjából tesztelni kell. Az ehhez szükséges lépéseket az Informatikai fejlesztés biztonsági feladatai és dokumentumai c. táblázatban (4. sz. melléklet d) része: A rendszer használatba vétele) összefoglaltak szerint kell elvégezni.

A biztonsági teszt-feltételeket nem teljesítő rendszert alkalmazásba venni, üzemeltetni szigorúan tilos. A tesztelési folyamatok irányítására – amennyiben az üzleti tulajdonos szerint indokolt – egy szervezetet kell létrehozni, aminek a vezetője az üzleti tulajdonos által kijelölt teszt-menedzser. Tagjai továbbá a rendszer méretétől (bonyolultságától) függő létszámban a teszt-tervező(k), tesztelő(k), értékelő(k). A tesztelésbe a felhasználó környezetéből is be kell vonni személyeket, akiket az üzleti tulajdonos jelöl ki. A tesztelés végrehajtására a teszt-menedzser (vagy az üzleti tulajdonos) által jóváhagyott teszt tervet kell készíteni. Az általános teszt terv készítője minden esetben a rendszer szállítója, míg a biztonsági tesztet a rendszer funkcióinak megfelelően a Társaság Biztonság szervezete készíti. Ennek legfőbb elemei a következők:

- a teszt céljainak meghatározása,
- a teszt lépéseinek meghatározása,
- a rendszer tesztelendő elemeinek behatárolása,
- tesztelési mód, teszt környezet, teszt adatbázis meghatározása,
- fentiekhez szükséges tesztelési szervezet kialakítása, személyek meghatározása, szerepkörök, felelősségi leírása,
- tesztek értékelési módszerének kialakítása,
- teszteredmények megfelelőségi kritériumainak definiálása,
- dokumentálási feladatok meghatározása,
- ütemterv meghatározása.

A tesztelés tervét a rendszertervvel párhuzamosan kell elkészíteni, mivel a biztonsági követelmények addigra már ismertek. Az informatikai tesztelésekkel párhuzamosan meg lehet kezdeni a biztonsági tesztelési eljárásokat, támogatva ezzel az üzleti tulajdonos rendszerrel szembeni biztonsági elvárásainak időbeni teljesülését. A tesztek (modul-, integrációs-, rendszer-, teljesítmény-, stb.) eredményét a 8. sz. melléklet szerinti Biztonsági tesztelési jegyzőkönyveken kell rögzíteni és a rendszerdokumentáció részeként meg kell őrizni.

A rendszer csak akkor vehető használatba, ha rendelkezésre áll a(z):

- üzleti tulajdonos nyilatkozata a biztonsági osztályba sorolásról (14. számú melléklet),
- üzleti tulajdonos nyilatkozata a maradó kockázatok felsorolásáról és elfogadásáról, (14. számú melléklet),
- felhasználóknak szánt Kezelési kézikönyv az összes kezelési szintre, benne olyan funkciókkal, mint az informatikai biztonsági eseményekre való reagálás és az informatikai működésfolytonosság biztosítása,
- Üzemeltetési kézikönyv,
- Rendszerszintű Informatikai Biztonsági Szabályzat (kisebb rendszerek rendszertervében informatikai biztonsági fejezet), ami tartalmazza a rendszer összes konkrét védelmi intézkedését,
- rendelkezésre szempontjából fokozott illetve kiemelt biztonsági osztályú rendszerek esetében az Informatikai Működésfolytonossági Terv és a Változáskezelési Eljárásrend,
- biztonsági tesztfeltételeknek való megfelelés jegyzőkönyve,
- minősített rendszer független auditortól származó megfelelőségi bizonyítványa a 4.10.2. b) pont szerint.

4.9. Informatikai működésfolytonosság tervezése

Működési hibák, különböző fokozatú rendkívüli állapotok (közte akár természeti katasztrófa) által okozott károk enyhítésére, illetve a feldolgozó képesség bármely okból bekövetkező hosszabb kiesésének fedezésére a Társaság valamennyi, a rendelkezésre állás szempontjából fokozott és kiemelt biztonsági osztályba sorolt informatikai rendszerének – annak kiterjedésétől függetlenül – rendelkeznie kell az Informatikai Működésfolytonossági Tervvel. A tervezés olyan hibák és jelenségek kezelésére szolgál, amelyek a rendszer működése során gyakran előfordulhatnak a helytelen munkavégzésből, figyelmetlenségből, vagy a technikai körülmények előnytelen változásaiból, személyek változásából, illetve elháríthatatlan okból (pl. természeti katasztrófa).

Az informatikai működésfolytonossági tervezést az üzleti tulajdonos irányítja.

Első lépésben meg kell határoznia a rendszer azon kiesési idejét, amely mellett a rendszer által támogatott és kiszolgált üzleti folyamat megszakadása számára üzletileg még elviselhető, és aminek leteltével életbe kell léptetnie a biztonsági események kezelésére

szolgáló intézkedéseket. A tervezés során nem csak az informatikai, hanem az üzleti folyamatokat is figyelembe kell venni. Az informatikai működésfolytonosság tervezése során azonosítani kell azokat az eseményeket, melyek befolyásolhatják az adott rendszer rendeltetésszerű működését. Ezek lehetnek például hardver meghibásodások, adatátviteli útvonalon történő zavar, tartós szakadás, programhiba, vagy tűzeset, vízkár.

A tervezés során az alábbi kulcsfontosságú elemek, szempontok érvényre jutását biztosítani kell:

- fel kell készülni mindazokra a kockázatokra, melyek bekövetkezése reális, és befolyásolhatja az üzleti folyamatokat,
- differenciáltan kell tervezni: fel kell készülni mind az egyszerűbb, mind a bonyolultabb incidensek kezelésére, beleértve a katasztrófahelyzetet is,
- figyelembe kell venni, hogy a katasztrófaesemény a működésfolytonosságot hátrányosan befolyásoló, azt különböző mértékben érintő tényezők legdurvább előfordulási módja ugyan, de csak egy a tényezők sorában,
- ki kell alakítani a terv szinkronját az üzleti stratégiához, biztosítani kell alkalmazkodását a változó jogi előírásokhoz,
- megfelelő stratégiát kell kidolgozni, hogy a kockázatok minimálisak legyenek,
- meg kell állapítani a felelősségi területeket, a követendő eljárási tematikát,
- meg kell határozni a reagálási és a helyreállítási stratégiát, annak idejét,
- minél rövidebb terjedelmű, működési zavarral terhelt környezetben dolgozó (esetleg katasztrófa-helyzetben pánik-közeli állapotba került) munkatársak számára is könnyen érthető, elméleti fejtegetéseket teljes mértékben mellőző feladatleírást, cselekvési tervet kell kialakíttatni, ami egyértelműen és kizárólag a végrehajtandó feladatokat tartalmazza, meghatározva azok sorrendjét és felelőseit,
- valamennyi részelemnek – függetlenül az üzleti tulajdonos mindenre kiterjedő biztonsági felelősségétől – további felelőse kell, hogy legyen, aki felel a felelősségi körébe tartozó rendszerelemek működésének helyreállításáért, annak feladatait ismeri és készség szintjén begyakorolta,
- biztosítani kell a munka végzését – az adott üzleti folyamat megszakítatlanságát – egy a kérdéses folyamat működését gátló rendkívüli körülmények fennállása idejére, helyettesítő munkaerő bevetése, munkaerő átcsoportosítása, kézi nyilvántartások vezetése, csökkentett szolgálatellátás bejelentése, a kiesett elem pótlása, stb. útján.
- a tervet időszakonként felül kell vizsgálni és a szükségletnek megfelelően módosítani kell,
- a tervet évente oktatni kell, elsajátításáról évente gyakorlati próbával kell meggyőződni,
- ki kell dolgozni a média kezelésének, a Társaság szóvivőjével való együttműködésnek a szabályait.

4.9.1. A tervezés keretrendszere

Az Informatikai Működésfolytonossági Terv általános tematikáját a 9. sz. melléklet tartalmazza. A dokumentumnak szoros logikai kapcsolatban kell állnia az érintett rendszer informatikai biztonsági rendszertervével, a Rendszerszintű Informatikai Biztonsági Szabályzatával, és a felhasználói kézikönyvvel. A megadott tematikai vázlatot az alábbi tervezési szempontok figyelembe vételével kell alkalmazni:

- rögzíteni kell a meglevő és a helyreállításra igénybe vehető erőforrások térbeli és minőségi helyzetét,
- fel kell mérni azokat a környezeti szereplőket, akiket / amelyeket valamilyen formában értesíteni, vagy bevonni kell egy rendkívüli helyzet esetén (pl. informatikai szolgáltató, közvetlen vezető, üzleti tulajdonos, rendszergazda, tűzoltóság, rendőrség, katasztrófavédelem, írott és elektronikus sajtó),
- a kockázatoknak megfelelően tartalék erőforrásokat kell feltárni, elemezni kell a rendszer külső beszállítóinak ilyen esetekre tartalékolt szolgáltatásait, erőforrásait,
- meg kell határozni a műszaki helyreállítás lehetőségeit (az eszközök üzembe történő visszaállítása, tartalék eszközök üzembe helyezése, hideg / melegtartalék kezelése, alternatív helyszín igénybe vétele) figyelembe véve a rendszerre vonatkozó kapacitásigényt,
- el kell végezni a tartalék helyszín megfelelőségi vizsgálatát,
- konkrétan tervezni kell:
  - a helyreállítási fázisok részfelelőseinek folyamatos beszámoltatási kötelezettségét,
  - a tervbe felvett feladatok időigényét,

- alternatív megoldásokat, szükségmegoldások lehetőségét,
- ki kell alakítani az érintettek listáját, rögzíteni kell elérhetőségüket (cím, telefonszám), és a listát az üzemeltető személyzet számára könnyen elérhetővé kell tenni,
- a szűkebb körű személyi állomány – vezetői állomány vagy speciális szakterületek (riasztásához szükséges címadatokat,
- a teljes munkavállalói állomány név- és címlistáját szervezeti egységenkénti és szakmánkénti csoportosításban (nagy létszámú vagy több telephelyű intézményeknél a szervezeti egységenkénti, illetve telephelyenként külön, egy időben történő riasztást célszerű tervezni),
- a riasztás módját (telefon, mobiltelefon, távirat stb.) többféle változat kidolgozásával, számolva az egyes kommunikációs rendszerek katasztrófa esetén bekövetkező működésképtelenségével,
- az alternatív kiértesítési lehetőségeket (telefon mellett mobiltelefon, gépkocsival történő kiértesítés, helyi elektronikus média),
- a riasztást, berendelést (kiértesítést) végrehajtó személy(ek) kijelölését, feladatainak meghatározását,
- a kiértesítés rendjét, beleértve a riasztási lánc megszakadása vagy megszakadása veszélye esetén szükséges teendőket is,
- az értesítendő vezetői állomány - elérhetőségük hiányában az őket helyettesítő személyek név- és címlistáját,
- a riasztás végrehajtásának, illetve a berendeltek beérkezésének normaidejét,
- a beérkezők fogadását és feladataik kiadásának felelősét.

4.9.2. A terv felülvizsgálata és karbantartása

Az adott rendszer Informatikai Működésfolytonossági Tervét annak üzleti tulajdonosa köteles évente vizsgálatnak alávetni és szükség esetén módosítani. Ezt indokolja, hogy előfordulhatnak hibás feltételezések, személyi változások, vagy technológiai, rendszertechnikai módosítások. A felülvizsgálatok során nemcsak arra kell választ adni, hogy mi a módosulás, hanem ismerni kell annak időbeliségét, hatását és következményeit is.

4.9.3. A rendszerek és a programok működési zavarainak értékelése

A Társaság minden szerverén és munkaállomásán, (amennyiben a működtető szoftver ezt lehetővé teszi) folyamatosan naplózni és figyelni kell a rendszerek esetleges hibaüzeneteit. A hibaüzenetek fontosságát az informatikai működésfolytonosság fenntartásában a felhasználókkal is tudatosítani kell.

Az eseményeket típus, terjedelem, általuk okozott károk, helyreállítási költségek, alapján az üzleti tulajdonosnak évente elemeznie, értékelnie kell. Az elemzés alapján – szükség esetén – kezdeményeznie kell az információvédelmi szakterületnél jelen szabályzat, illetve saját hatáskörében az adott rendszer Informatikai Működésfolytonossági Tervének és RIBSZ-ének a korszerűsítését.

4.10. Megfelelés a jogszabályoknak

4.10.1. A jogszabályi előírások betartása

Az Informatikai Biztonsági Szabályzat alkalmazása során bevezetett védelmi intézkedések nem ütközhetnek büntetőjogi vagy polgári jogi előírásokba, nem eredményezhetik a Társaság törvényes, szabályozói vagy szerződéses kötelezettségének a megszegését. A Társaság informatikai kapcsolatainak biztosítására csak olyan technikai és adminisztratív intézkedések engedélyezhetőek, illetve valósíthatóak meg, amelyekkel a jogszabályi és egyéb előírásoknak megfelelően biztosítják az informatikai infrastruktúra védelmét.

A szabályzat kialakításánál a 10. sz. mellékletben felsorolt jogforrások és előírások normái voltak irányadók. Az informatikai biztonság irányítása és megvalósítása során az abban részt vevőknek kiemelt figyelmet kell fordítani a Büntető Törvénykönyvbe felvett számítástechnikai bűncselekményi tényállásokra (11. sz. melléklet).

Az informatikai rendszerekkel kezelt és feldolgozott
- titokká minősített adatok titokvédelmét a Társaság titokvédelmi felügyelője a Társaság titokvédelmi szabályzatai szerint,
- személyes adatok védelmét a Társaság belső adatvédelmi felelőse a Társaság Adatvédelmi Szabályzata szerint látja el.

4.10.2. Az informatikai biztonság megfelelőségi felülvizsgálata

A Társaság informatikai biztonsági szintjét folyamatosan és célirányosan ellenőrizni, felügyelni kell. Annak elbírálását, hogy az informatikai folyamatok gyakorlata megfelel-e a mindenkori tárgybani jogforrásoknak, az informatikai biztonság megvalósítását végző személyektől, szervezeti egységektől független apparátusra kell bízni. A biztonsági felügyelet több szinten valósul meg:

a) az információvédelmi szakterület munkaszervezete folyamatosan, napi szaktevékenysége részeként, rutinszerűen ellenőrzi a rendszereket, felügyeli a rendszerek biztonságának megvalósításában feladattal megbízott szervezeti egységi vezetőknek és személyeknek a rendszerbe jelen szabályzattal beépített biztonsági mechanizmusaival kapcsolatos tevékenységét,

b) a Társaságon kívüli, független szakértők megbízásával külső auditálást kell végeztetniük az érintett rendszerek üzleti tulajdonosainak az alábbi esetekben:
- fokozott biztonsági osztályba sorolt rendszereknél a használatba vételt megelőzően,
- kiemelt biztonsági osztályba sorolt rendszereknél a használatba vételt megelőzően, majd 2 évenként rendszeresen.

4.10.3. Az informatikai biztonsági szabályok oktatása

4.10.3.1. Vezetők informatikai biztonsági képzése

Az oktatás célja, hogy a Társaság vezetői felfrissítsék és aktualizálják azon szabályzókra vonatkozó ismereteiket, amelyeket az informatikai biztonság területén figyelembe kell venniük vezetői munkájuk során. Vezetői szinten a terület alapos megismerése azért kötelező, mert a szabályzat számukra kiemelt, a munkatársakénál nagyobb felelősséget és jóval több feladatot ír elő. Célcsoportok:

- az összes alkalmazás (informatikai biztonsági szempontból értelmezett) üzleti tulajdonosa,
- a titokvédelmi minősítésre feljogosított vezetők,
- a munkáltatói jogkört gyakorló vezetők,
- az előző három kategóriába nem tartozó vezetők.

A felsoroltakat évente legalább egy alkalommal, 1 óra időtartamú informatikai biztonsági oktatásban kell részesíteni.

4.10.3.2. Felhasználók informatikai biztonsági képzése

A felhasználóknak a munkakörüknek megfelelően ismerniük kell a biztonsági eljárások alkalmazását és az információfeldolgozó lehetőségek korrekt használatát, hogy ezzel is a minimálisra csökkentsék a biztonsági kockázatokat.

Főszabályként belépéskor biztonsági alapképzést, majd évente fél órában utánképzést kell lebonyolítani a felhasználók részére. A biztonsági képzések tananyagát a korábban már említett, Felhasználók biztonsági kötelezettségei c. segédlet képezi, amit az adott munkaterület speciális igényei szerinti előadásokkal lehet kiegészíteni. Mind az alapképzés, mind az éves utánképzés a segédlet önálló tanulmányozásával is elvégezhető. Utóbbi megtörténtét a munkáltatói jogkörgyakorló köteles a biztonsági vezetőnek írásban visszaigazolni.

5.0. HIVATKOZÁSOK, BIZONYLATOK, MÓDOSÍTÁSOK, HATÁLYON KÍVÜL HELYEZÉSEK

5.1 Hivatkozások

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról,
- 2012. évi C. tv. a Büntető Törvénykönyvről,
- 16/2011. (IX. 20. MÁV-START Értesítő 5.) VIG sz. utasítás a szerződéskötések rendjéről,
- 19/2008. (IV.11. MÁV Ért. 6.) VIG. sz. vezérigazgatói utasítás a MÁV-START Zrt. Adatvédelmi Szabályzata,
- 20/2008. (IV.11. MÁV Ért. 6.) VIG. sz. vezérigazgatói utasítás a MÁV-START Zrt. Üzletititok-védelmi Szabályzata,
- 54/2008. (X.15. MÁV-START Ért. 18.) VIG. sz. vezérigazgatói utasítás a MÁV-START Zrt. Vagyonvédelmi szabályzatáról,
- 12/2011. (IX. 26. MÁV-START Ért. 6.) sz. általános gazdálkodási vezérigazgató-helyettesi utasítás a távmunka működtetéséről a MÁV-START Zrt.-ben,

- MÁV Gépészet Zrt. 30/2009. (12.01.) számú VIG utasítás Informatikai Biztonsági Szabályzat.

5.2 Bizonylatok
Nincsenek.

5.3 MÓDOSÍTÁSOK
Nincsenek.

5.4 Hatályon kívül helyezések
Az utasítás hatályba lépésével egyidejűleg hatályát veszti a 10/2010. (IV. 2. MÁV-START Ért. 10.) VIG. sz. vezérigazgatói utasítás a MÁV-START Zrt. Informatikai Biztonsági Szabályzata.

6.0. HATÁLYBA LÉPTETÉS
Jelen szabályzat előírásait a MÁV-TRAKCIÓ Zrt-nek és a MÁV-GÉPÉSZET Zrt-nek a MÁV-START Zrt.-be történő beolvadása napjától kezdődő hatállyal kell alkalmazni.

7.0. MELLÉKLETEK
1. sz. Felhasználók biztonsági kötelezettségei
2. sz. Kárérték és kárgyakoriság besorolási táblázata, kockázati mátrix
3. sz. Informatikai biztonsági nyilatkozat
4. sz. Informatikai fejlesztés biztonsági feladatai és dokumentumai
5. sz. Kockázatelemzés és kockázatkezelés
6. sz. Informatikai biztonsági rendszerterv vázlata
7. sz. Minősített biztonsági osztályok követelményei
8. sz. Biztonsági tesztelési jegyzőkönyv
9. sz. Informatikai Működésfolytonossági Terv vázlata
10. sz. Az IBSZ tartalmát meghatározó vagy befolyásoló jogforrások
11. sz. Számítástechnikai bűncselekmények a Büntető Törvénykönyvben
12. sz. Rendszerszintű Informatikai Biztonsági Szabályzat vázlata
13. sz. Felhasználó beosztottal rendelkező közvetlen vezető informatikai biztonsági jellegű feladatai
14. sz. Nyilatkozat a maradvány kockázatok elfogadásáról és a rendszer biztonsági osztályba sorolásáról

Ungvári Csaba s.k.
vezérigazgató

1. sz. melléklet

Felhasználók biztonsági kötelezettségei

Jelen dokumentum célja, hogy biztosítsa minden felhasználó számára azokat a legfontosabb információkat, amelyek ismeretében a Társaság informatikai infrastruktúrája eredményesen, hatékonyan, és biztonságosan használható. A Társaság Informatikai Biztonsági Szabályzata szerint a Társaságnak azon munkavállalója, aki munkája ellátásához számítógépet használ (másképpen: felhasználó) köteles az itt felsorolt szabályokat ismerni, munkájában alkalmazni és az informatikai biztonság fenntartásában közreműködni.

Bevezetés

A Társaság rohamosan növekvő mértékben alkalmaz számítógépes rendszereket az üzleti tevékenységével összefüggő nyilvántartási, adatfeldolgozási feladatokra, de belső és külső elektronikus kommunikációra is. A rendszerek a velük végzett napi munka során különböző biztonsági fenyegetéseknek vannak kitéve, amelyek ellen a Társaság védelmi rendszert működtet. Informatikai biztonsági szempontból elsősorban az adatok és feldolgozórendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése a fő feladat.

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

Az informatikai eszközök és rendszerek folyamatos működőképessége és ennek során a biztonsági követelmények érvényesülése fontos üzleti érdek, így minden érintett kötelessége ennek szellemében tevékenykedni.

1. Biztonsági ismeretek, felelősségtudat

A Társaság munkavállalói, mint felhasználók felelősséggel tartoznak az általuk használt személyi számítógép és tartozékai, továbbá az informatikai rendszerek (számítógépes programok) biztonságának megőrzéséért. Kötelesek a használatra vonatkozó biztonsági szabályokat megismerni, azokat a tevékenységüknek megfelelő esetekben alkalmazni és ennek során a tőlük elvárható gondossággal ellenőrizni az alkalmazott biztonsági funkciók helyes működését.

2. Egyéni felelősség

a) A felhasználók elszámoltathatók az informatikai rendszerekben végzett tevékenységükért. A felhasználók kötelesek mindent megtenni annak érdekében, hogy mások a nevükben illetéktelenül ne tevékenykedhessenek. Kötelesek betartani a jelszóválasztási és változtatási szabályokat. A jelszót azonnal meg kell változtatni, ha a felhasználó megtudja, vagy gyanakszik rá, hogy az más számára ismertté vált.
b) A felhasználók nem oszthatják meg senkivel, és nem árulhatják el senkinek a hozzájuk rendelt felhasználói azonosítókat és jelszavakat, továbbá más nevében nem léphetnek be a rendszerbe.
c) Végfelhasználói alkalmazások (a felhasználók által fejlesztett és / vagy használt, legtöbbször általános célú szoftver eszközökön alapuló megoldások, pl. Excel-táblák, makro-programok, SQL lekérdezések, kis adatbázisok) nem tekinthetők informatikai alkalmazásnak.

A vezetők az általuk irányított területen felelősek a végfelhasználói alkalmazásoknak a biztonsági előírásokkal összhangban levő használatáért. Az ezekkel előállított adatok, eredmény, stb. megbízhatóságának ellenőrzése a felhasználó felelőssége.

d) A felhasználók kísérjék figyelemmel a PC munkaállomásukat érintő üzemeltetési, karbantartási tevékenységet, legyenek jelen ezek végzése során. Amennyiben az eszközök működésében váratlan változást tapasztalnak, tájékoztassák közvetlen vezetőjüket.
e) A felhasználók a jelszavuk által aktivált berendezésüket rövid időre sem hagyhatják felügyelet nélkül. Ki kell lépniük a használt alkalmazásokból, illetve kötelesek aktivizálni a PC munkaállomás jelszavas védelemmel ellátott képernyővédő funkcióját, ha munkahelyüket – akár rövid időre is – elhagyják, vagy egyéb módon gondoskodjanak a számítógép mások általi használatának megakadályozásáról (pl. a helyiség bezárása).
f) Köteles tájékoztatni közvetlen vezetőjét a munkaviszonyában bekövetkező változásokról.
g) Felhasználó a Társaság semmilyen adatát, dokumentumát és egyéb információit idegen – a Társasággal szerződéses viszonyban nem álló - szolgáltató eszközén nem helyezheti el, idegen szolgáltató eszközén nem kezdeményezhet felhasználói regisztrációt.

3. Felhasználói jogosultság

a) A felhasználók a részükre meghatározott munka elvégzéséhez szükséges mértékű hozzáférést kapnak az informatikai rendszerekhez “a szükséges minimális jogosultság” elvének alapján, az adott rendszerre vonatkozó felhasználó-adminisztrációs eljárásoknak megfelelően. A jogosultság érvényessége köthető időszakhoz is.
b) A felhasználók kötelesek a vezetőjük által engedélyezett (jogosultsági) határokon belül dolgozni és nem tehetnek kísérletet azon rendszerek, alkalmazások, funkciók, adatok elérésére, amelyekre nincsenek feljogosítva.
c) A felhasználók csak indokolt esetekben kaphatnak rendszergazdai (adminisztrátori) jogosultságot.

4. Jelszavak használata

A Társaság informatikai rendszereit használó valamennyi felhasználónak a következő jelszóhasználati szabályokat kell betartania.

a) A felhasználónak tudatában kell lennie, hogy mindazon műveleteket, melyeket az ő azonosítójával és jelszavával bárki végrehajt, az informatikai rendszer az ő „terhére” könyveli el. Ezért a jelszavait bizalmasan kell kezelnie, azokat más személyeknek nem adhatja meg, nyilvánosságra nem hozhatja, köteles azok titkosságát megőrizni. A felsoroltakért személyesen felelős.
b) A jelszó jellemzői (hossz, bonyolultság, cserélés periódusa, stb.) rendszerenként változhatnak, de alapszabály, hogy a jelszó nem egyezhet meg a felhasználói azonosítóval.
c) A jelszó kívülálló számára ne legyen egyszerűen kitalálható, ne tartalmazzon a felhasználóra, vagy hozzá közel álló személyekre, tárgyakra, stb. utaló információkat (pl. neveket, telefonszámokat, születési dátumokat, kocsija forgalmi rendszámát, kedvenc háziállata nevét, stb.
d) A felhasználó nem adhat meg a hálózati bejelentkezésére használt jelszóval megegyező jelszót az általa használt informatikai rendszerekben.
e) A jelszavakat – a biztonsági másolat kivételével – nem szabad felírni, papíron tárolni. Amennyiben ez elkerülhetetlen (pl. a biztonsági másolat, vagy a kezdeti jelszó), akkor gondoskodni kell a jelszó zárt borítékban, a közvetlen vezetőnél történő, biztonságos tárolásáról.
f) Amennyiben a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal le kell azt cserélnie. Ha ez a jelszópolitika miatt nehézségekbe ütközik (pl. belül van a cserére minimálisan előírt időszakon), kérje a Biztonság segítségét.

g) Ha a jelszópolitikától eltérő időpontban szükséges a hálózati bejelentkezési jelszó cseréje, akkor a közvetlen vezetőnek a hálózati üzemeltetőhöz kell e-mailt küldenie és a 4.7.2. A felhasználói jelszó kezelése pont szerint kell eljárni.
h) a felhasználó köteles gondoskodni arról (pl. a billentyűzet ideiglenes eltakarásával), hogy más ne láthassa meg az általa beírt jelszót.
i) A részére generált első jelszót, továbbá a jelszómódosításra felhívó rendszerüzenetek után az addig érvényes jelszavát a felhasználó a legelső bejelentkezése alkalmával köteles módosítani.

5. A Társaság eszközeinek használata

a) A felhasználók nem jogosultak a Társaság infokommunikációs erőforrásai – az informatikai alkalmazások (szoftvertermékek) a számítógépes hálózat, az Internet, a munkaállomások és az egyedi PC-k, továbbá a számítástechnikai adathordozók (mágneslemez, CD ROM, stb.) – személyes célú használatára.
b) A számítógépes erőforrásokhoz való hozzáférés és azok használata kizárólag megfelelően azonosított, hitelesített és jogosított felhasználók számára engedélyezett.
c) A Társaságnál csak a hivatalos csatornákon keresztül beszerzett, elfogadott és installált PC hardver és szoftver, illetve adathordozó (pl. CD, pen-drive) használható.
d) A felhasználó nem jogosult a PC hardver önálló installálására vagy módosítására (pl. modem, külső tárolóeszköz telepítése). A Társaság munkaállomásain a szoftverek telepítését és karbantartását szerződésben megbízott üzemeltető szervezet végezheti.
e) Bemutató céljára tilos olyan PC-t használni, amely képes minősített biztonsági osztályú üzleti alkalmazás elérésére.
f) A munkaviszony megszűnése, a munkakör megváltozása, vagy más, a közvetlen vezetője által támasztott igény esetén a felhasználónak minden, számára a továbbiakban nem szükséges eszközt és információs erőforrást vissza kell szolgáltatnia.
g) A felhasználói munkaállomásokhoz bármilyen telekommunikációs eszközt (pl. modem, mobiltelefon) vagy az informatikai szabályzatokban engedélyezetten túlmenő hardver eszközt csatlakoztatni a közvetlen vezető által a Biztonság szervezetétől e-mail-ben igényelt, kifejezett engedéllyel szabad.
h) A Társaság informatikai hálózatához és számítógépeihez saját tulajdonú informatikai berendezésekkel (pl. pen-drive, külső merevlemez vagy SSD, okostelefon) csatlakozni tilos.
i) Ha a munkavállaló munkaviszonya bármilyen okból megszűnik, az esetlegesen bármely eszközön tárolt személyes adatait nyilatkozat kitöltése (AVSZ. 2. számú melléklet) mellett törölnie kell. A számítógépen csak azok az adatállományok maradhatnak, melyek a munkakört a továbbiakban betöltő másik személy munkavégzéséhez szükségesek.

6. Az adatok érzékenysége

a) A felhasználó felelős a rendszerek használata során tudomására jutott titokká minősített adatok (üzleti titok), továbbá a belső és a személyes adatok megőrzéséért.
b) Titokká minősített adatok külső tárolóra másolása csak az erre vonatkozó, kifejezetten megengedő szabályok szerint történhet. Az ilyen információt tartalmazó eszközt használaton kívül a vonatkozó biztonsági szabályok szerint kell tárolni.
c) A felhasználók senki előtt nem fedhetik fel a titokká minősített információt, kivéve, ha azt a rendszer (információ) tulajdonosa engedélyezi. Ebbe beletartoznak a Társaságra, valamint ügyfeleire, informatikai rendszerére és szoftverfejlesztésére, termékeire és szoftver liszenszeire vonatkozó technikai és üzleti információk.
d) Az informatikai biztonsági intézkedéseket és a Társaság erre vonatkozó belső szabályzatait bizalmasan kell kezelni.
e) Titokká minősített (legalább üzleti titkot tartalmazó) információkat külső félnek elektronikus úton kizárólag a Társaság titokvédelmi szabályzataiban leírt módon szabad küldeni.

f) Minden, a felhasználónak a számítógépekhez való hozzáféréséhez szükséges azonosító, jelszó, telefonszám, valamint egyéb, a számítógépes erőforrásokhoz való "hozzáférési lehetőség" a felhasználó tulajdona és titka. Az ilyen hozzáférési lehetőség birtokosa felelősségre vonható ennek jogtalan vagy gondatlan használatáért, felfedéséért.
g) A felhasználók a belső adatok védelmére kötelesek külön intézkedéseket alkalmazni a kapott lehetőségeken belül, vagy külön intézkedéseket kérni (pl. diszk-zárakat, az érzékeny fájlok és üzenetek titkosítását, a könyvtárak és fájlok külön jelszavas védelmét).
h) Az általa használt elektronikus adathordozókat (pl. mágnesszalag, hajlékony- és merevlemez, újraírható CD, DVD) a szokásos eszközökkel, helyreállíthatatlan módon a felhasználónak le kell töröltetnie a Biztonság szervezet közreműködésével újrafelhasználás vagy selejtezés előtt. A titokká minősített adatokat tartalmazó szalagokat, lemezeket, stb. selejtezés előtt fizikailag meg kell semmisíteni, vagy más módon lehetetlenné kell tenni az adatok visszaállíthatóságát.
i) A kinyomtatott érzékeny adatokat tartalmazó anyagokat, a feleslegessé vált, érzékeny információt tartalmazó papírokat, mint pl. a képernyők kinyomtatott képeit, táblázatokat, levelezések és szabályzatok másolatait stb. a vonatkozó iratkezelési, iratmegsemmisítési szabályok szerint kell kezelni.

7. Adatok biztonsági mentése

a) A helytakarékos tárolás elvének megfelelően a felhasználók kötelesek a nem szükséges anyagaikat folyamatosan törölni a könyvtáraikból, továbbá a közös használatú anyagokat közös elérésű könyvtárakban kell kezelni.
b) A külön engedéllyel helyben, különféle elektronikus adathordozón tárolt adatok biztonsági másolatának elkészítéséről a felhasználók kötelesek gondoskodni.
c) Minden munkavállaló a Társaság központi szerverén, az úgynevezett 'start-fs\users' O: meghajtón kap tárolási területet, erre a (naponta központilag mentett) területre köteles felmásolni az általa használt számítógépen helyben tárolt adatokat, hogy azok rendelkezésre állása biztosított legyen. A másolást célszerű legalább hetente elvégezni. Ezen tevékenység elmulasztása esetén, ha bármilyen adatvesztés történik, annak felelőssége a munkavállalót terheli.
d) A biztonsági mentések adathordozóit az erre feljogosított felhasználónak a vonatkozó előírásoknak megfelelő módon kell tárolni (eredeti helyszíntől földrajzilag távol, tűzvédett, kulccsal zárható stb. helyen).
e) Az informatikai rendszerek rendelkezésre állásában minden felhasználó érdekelt. Az informatikai rendszer működésképtelensége esetén minden felhasználó felelősséggel tartozik a szolgáltatások helyreállításának támogatásáért, a biztonsági mentések megfelelő használatáért.

8. Vírusok elleni védelem

a) Az installált vírusvédelmet tilos hatástalanítani. A vírusvédelemmel 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 közvetlen vezető útján az információvédelmi szakterületnek.

9. Szoftver tulajdonjog

a) A Társaság által beszerzett szoftvereket és a hozzájuk tartozó dokumentációkat tilos másolni, kivéve, ha az biztonsági másolat készítése céljából szükséges, vagy arra a szoftver-terjesztő / fejlesztő egyértelmű írásos engedélyt ad. Ezt a másolatkészítést az informatikai szakterület végzi és dokumentálja. Egyetlen termék többszörös használata esetén a szoftver csak a liszensz-megállapodásban rögzített darabszámban és módon használható.

b) A szerzői jogok megsértése törvénybe ütköző cselekmény, ami felelősségre vonáshoz vezethet és a felhasználó elleni büntetőeljárás megindítását eredményezheti. Ha kétségek merülnek fel a szoftver szerzői jogai felől, akkor az IT terület szoftver liszensz-nyilvántartásért felelős munkatársának segítségét kell kérni. A felhasználók:

- nem installálhatnak, nem karbantarthatnak, vagy nem tölthetnek le szoftvert (beleértve az ún. szabad-felhasználású, freeware, shareware, stb. programokat is) a Társaság munkaállomásaira,
- a Társaság munkaállomására felinstallált szoftvert nem másolhatják más helyen történő használat céljából.

A tilalom nem vonatkozik azokra a kulcsfelhasználókra, rendszeradminisztrátorokra, stb., akiknek a felhasználók informatikai támogatása munkaköri kötelességük, de a letöltéseket, másolásokat minden esetben a munka céljának kell indokolnia.

10. Berendezés-védelem

a) A felhasználóknak szállítás közben a lehetőségei határain belül személyesen kell vigyázniuk hordozható személyi számítógépükre, meg kell óvniuk fizikai állapotát, lehetőségeiken belül gondoskodniuk kell az eltulajdonítás megakadályozásáról.
b) A munkaállomás átadásakor a felhasználó az információvédelmi szakterület útján köteles gondoskodni a felelősségi körébe tartozó adatoknak a PC-ről való ún. biztonságos törléséről, vagy az új géphasználónak dokumentált módon való átadásáról.
c) Selejtezésre leadott PC-ről minden adatot – beleértve az operációs rendszert is – biztonságosan törölni kell az információvédelmi szakterület bevonásával.
d) A hordozható számítógépeket (note-book, net-book, palm-top, PDA, okostelefon, i-PAD stb.), valamint a kivehető adattároló eszközöket (mágneslemezeket, CD/DVD-ket, szalagokat, kazettákat, stb.) használaton kívül, illetve irodán kívül biztonsági zárral zárható íróasztalban vagy szekrényben kell tartani. Személygépjárműben szállítva úgy kell elhelyezni, hogy ne legyen látható.
e) Kiemelten ügyelni kell arra, hogy ártalmas kód vagy vírus ne fertőzhesse meg a külső adattároló állományait, ezért a hordozható eszközbe helyezéskor induló kártevő-ellenőrzési eljárást tilos gátolni, vagy megszakítani.
f) A berendezésektől az ételt, italt távol kell tartani.

11. Területvédelem

A felhasználók kötelesek távol tartani a berendezéseiktől és adataiktól az oda hozzáférési jogosultsággal nem rendelkező személyeket, és közvetlen munkakörnyezetükben kötelesek kérdőre vonni az idegeneket.

12. Számítógépes munkavégzés hivatali helyiségen kívül

A Társaság kijelölhet olyan felhasználókat, akik a hivatali helyiségeken kívül is dolgozhatnak. Minden erre vonatkozó megállapodást írásban, a közvetlen vezetőnek és az alkalmazás üzleti tulajdonosának jóváhagyásával kell megkötni, amelyben rögzíteni kell:

a) a hivatali helyiségeken kívüli munkavégzés engedélyezési időszakát,
b) a munkavégzéshez az alkalmazott részére (otthonában) a Társaság által biztosított berendezések azonosítását, ill. a szükséges berendezések és anyagok átadási és elszámolási módját, továbbá,
c) hogy szükség van-e adatkapcsolatra, ill. rendelkezésre áll-e a megfelelő engedély (lásd a ”13. Munkavégzés távolról” pontot alább).

13. Munkavégzés távolról

Ez azt jelenti, hogy a Társaság alkalmazottja úgy éri el a megszokott munkakörnyezetét valamely külső helyről (pl. otthonról), mint ha ezt az irodájából tenné. Emiatt további biztonsági intézkedések szükségesek:

a) A felhasználónak megállapodást kell aláírnia, amelyben külön hangsúly esik a sajátos felelősségre, feltételekre és követelményekre. A távoli munkavégzéshez a közvetlen vezetőnek és az alkalmazás üzleti tulajdonosának az írásos megbízása szükséges.
b) Ha távoli hozzáférés létesítésére engedélyt ad a Társaság, fenntartja a jogot magának, hogy rendszeresen megvizsgálja a (tele)kommunikációs naplókat (logs), a hívások adatait, és szúrópróba szerinti ellenőrzést végezzen annak meghatározására, hogy a gyakorlati kivitelezés megfelel-e a vonatkozó előírásoknak.
c) A távoli munkavégzés esetén a titokká minősített adatokat rejtjelezni kell a továbbítás során, és – a biztonságos jelszó mellett – további hitelesítő eszközt (pl. token) kell alkalmazni.

14. Internet-használat

a) Az Internetre csatlakozás a Társaság belső hálózatára csatlakozó munkaállomásról kizárólag 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) A Társaság az Internet elérése során a felhasználói részére a munkavégzéséhez szükséges mértékű, még elégséges szintű hozzáférést biztosít. A Társaság a hozzáférést központilag korlátozza.
d) Az Internetről csak olyan állományok tölthetők le, amelyek a munkavégzéshez feltétlenül szükségesek.
e) A Társaság fenntartja magának a jogot a nem kívánatos, és a kártékony WEB-oldalak látogatásának megakadályozására. Minden olyan honlap (erotikus, on line játékok, közösségi portálok, on line rádiók stb.) használata tilos, ami veszélyeztetheti a Társaság informatikai rendszerét, vagy szűkítheti a sávszélességet, amivel akadályozzák más, a társaság részére kritikus (kiemelten fontos) rendszerek működését.
f) A Társaság fenntartja magának a jogot az összes Internetes tevékenység (beleértve a Web oldalak látogatását is) figyelemmel kísérésére, ezen tevékenység naplózására.

15. Elektronikus levelezés

Az elektronikus üzenetváltás (e-mail) a szervezet hivatalos kommunikációja; egy olyan szolgáltatás, amely az üzleti információcsere sebességének fokozásával a termelékenység növekedését, a hatékonyabb munkavégzést szolgálja.

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

a) Titokká minősített adatokat kizárólag a titokvédelmi szabályzatokban engedélyezett módon szabad tárolni, illetve továbbítani.
b) Az elektronikus üzenet vagy a csatolt anyag tömörítése (pl. WinZip-pel) és jelszavas védelme nem helyettesíti a magas szintű titkosítást.
c) Elektronikus levél jogi következményekkel járó kötelezettség vállalására – kifejezett felhatalmazás nélkül – nem használható.
d) Az elektronikus üzenet üzleti kommunikációra szolgál, nem használható személyes üzenetek közvetítésére. Az elektronikus levelezőrendszeren továbbított üzenetek a Társaság tulajdonát képezik. A Társaság fenntartja magának a jogot azok tartalmának vizsgálatára.
e) Tilos a bejövő üzenetek automatikus továbbítása Társaságon kívüli e-mail címekre.

f) Az elektronikus levél általában rövid üzenetek továbbítására szolgál. A sok személynek (pl. több, vagy nagy létszámú szervezeti egység, vagy projekt-team) címzett, vagy a mérete folytán várhatóan nagy szerverterhelést / vonalforgalmat eredményező elektronikus üzenetet a rendszergazda útján és ütemezésében kell – lehetőleg munkaidőn kívül – küldeni. Korlátozni kell azok számát, akik ilyen üzenet küldésére jogosultak.

g) A felhasználó elektronikus postaládájának karbantartása (az időszerűtlen és szükségtelen üzenetek megsemmisítése) a levelesláda tulajdonosának feladata és felelőssége.

h) A levelesláda 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 levelesládához a megfelelő eljárás szerint, de ezt az indok megszűnésekor azonnal vissza kell vonnia.

i) A küldőnek ellenőriznie kell, hogy a cím, amelyre üzenetet küld korrekt, és az illető személy jogosult az információ kézhez vételére.

j) A közvetlen vezetőnek – és lehetőleg közvetlenül a Biztonságnak is – jelenteni kell minden törvénysértésre utaló, különösen a gyalázkodó, rasszista, és a kéretlen elektronikus levél érkezését.

k) A levelezés során az üzleti kommunikációhoz méltó hangnemet kell használni; a szöveg legyen világos, ne legyen túl formális vagy feleslegesen közlékeny. Kerülendő olyan üzenet küldése, amely zavarba ejtő lenne, ha valaki körbeküldené az egész szervezetnek. Ha egy személyt név szerint megemlít az üzenet, az illetőnek másolatot kell küldeni, ha az illető részéről elvárt vagy várható az üzenettel kapcsolatos bármilyen megnyilatkozás.

l) A levélre adott válaszban lehetőség szerint kerülni kell az összes előzmény visszaküldését. Csak az a személy kapjon választ, akinek konkrétan szól az elektronikus üzenet. Ha az üzenethez tartozó korábbi levélváltások is részei a levélnek, akkor valamennyi korábbi címzettnek is továbbítani kell a válaszlevelet.

m) A felhasználók nem adhatják ki munkatársaik e-mail címét, vagy összesített címlistákat.

n) Tilos lánc- vagy kéretlen elektronikus leveleket másoknak továbbítani, mivel a csatolt anyagokban könnyen terjedhetnek számítógépes vírusok és rosszindulatú kódok. Aki ilyet kap, az köteles az üzenetet – lehetőleg elolvasás nélkül – törölni. A Társaság fenntartja magának a jogot az ilyen üzenetek kézbesítésének megakadályozására.

o) Tilos olyan leveleket és azok mellékleteit megnyitni vagy elmenteni, amelyek ismeretlen helyről vagy személytől származnak. Ezeket a leveleket a felhasználó köteles olvasatlanul, azonnal törölni.

p) Magáncélú elektronikus üzenetek továbbítása a Társaság hálózatába kapcsolt munkaállomásról tilos mind a Társaságon belüli, mind azon kívüli címekre (pl. Freemail, Citromail, Vipmail, Iwiw, Skype, Gmail).

q) A felhasználó köteles a levelező rendszerben az olvasó ablak megjelenését tiltani az összes kategóriában (beérkező üzenetek, elküldött üzenetek, törölt üzenetek, stb.).

r) A felhasználó a társaság által biztosított informatikai eszközről külső szolgáltató által biztosított postafiókot nem nyithat meg (pl. Freemail, Citromail, Vipmail, Iwiw, Skype, Gmail).

s) A Társaság hivatalos elektronikus levelezésben QR kódoknak a használata - különös tekintettel a munkavállaló által elhelyezett aláírásában történő felhasználása - nem megengedett.

16. Az információbiztonsági események és gyenge pontok jelentése

a) A felhasználó köteles közvetlen vezetőjének – és lehetőleg közvetlenül a Biztonság szervezetének is – haladéktalanul jelenteni a biztonsági előírások megsértését, a biztonsággal kapcsolatban felismert gyengeségeket, adataik gyanított jogosulatlan megváltozását.

b) Sürgős vagy indokolt esetben (pl. több gép egyidejű kiesése, számítástechnikai eszközök nyilvánvaló fizikai sérülése, rendszergazda szokatlan tevékenysége) közvetlenül a biztonsági vezetőhöz és az információvédelmi koordinátorhoz lehet fordulni. Elérhetőségük:

Biztonság titkársága: tel.: (1) 14-60, fax: (1)18-21,
információbiztonsági koordinátor: tel.: (1) 18-48,

c) A szabályzatba foglalt előírások értelmezésével, végrehajtásával kapcsolatban az információvédelmi szakértőkhöz lehet e-mailt intézni, továbbá ide kell jelenteni azokat az eseményeket (pl. a munkaállomás rendellenes viselkedése, levélszemét tömeges megjelenése), jelenségeket (pl. gyenge pontok, vélt sebezhetőségek), igényeket (pl. rendkívüli jelszócsere), stb., amelyekben a szabályzat a Biztonság szervezetét jelöli meg. Elérhetőségük:

információvédelmi szakértők: e-mail: infovedelem@mav-start.hu

2. sz. melléklet

Kárérték és kárgyakoriság besorolási táblázata, kockázati mátrix

a) A potenciális fenyegető tényezők okozta kár osztályát a következő értékskála szerint kell meghatározni (a Btk.459. § (6) bekezdése alapján):

1 : jelentéktelen kár
- közvetlen anyagi kár: 0 - 50.000 Ft
- közvetett anyagi kár 1 embernappal helyreállítható
- nincs bizalomvesztés, a probléma a szervezeti egységen belül marad
- nem sérül titokvédelmi vagy adatvédelmi előírás
- testi épség jelentéktelen sérülése egy-két személynél

2 : kisebb kár
- ha kár értéke 50.000 forintot meghalad, de 500.000 forintot nem halad meg
- közvetett anyagi kár 1 emberhónappal helyreállítható
- társadalmi-politikai hatás: kínos helyzet a Társaságon belül
- belső (intézményi) szabályozóval védett adat sérül
- könnyű személyi sérülés egy-két személynél

3 : nagyobb kár
- ha kár értéke 500.000 forintot meghalad, de 5.000.000 forintot nem halad meg
- közvetett anyagi kár 1 emberévvel helyreállítható
- társadalmi-politikai hatás: bizalomvesztés a Társaság középvezetésében, bocsánatkérést az ügyfél felé és/vagy fegyelmi intézkedést igényel
- személyes adat, üzleti titok sérül súlyos következmények nélkül
- több könnyű vagy egy-két súlyos személyi sérülés

4 : jelentős kár
- ha kár értéke 5.000.000 forintot meghalad, de 50.000.000 forintot nem halad meg
- közvetett anyagi kár 1-10 emberévvel helyre állítható
- társadalmi-politikai hatás: bizalomvesztés a Társaság felső vezetésében, személyi konzekvenciák
- szolgálati titok sérül
- üzleti titok, személyes adat sérül jogi következményekkel
- több súlyos személyi sérülés vagy tömeges könnyű sérülés

5 : különösen nagy kár
- ha kár értéke 50.000.000 forintot meghalad, de 500.000.000 forintot nem halad meg
- közvetett anyagi kár 10-100 emberévvel helyreállítható
- társadalmi-politikai hatás: súlyos bizalomvesztés a Társaság felső vezetésén belül személyi konzekvenciával
- államtitok, szolgálati titok sérül, különleges személyes adatok súlyosan sérülnek
- egy-két személy halála vagy tömeges sérülések

6 : különösen jelentős kár
- ha kár értéke 500.000.000 forintot meghalad
- közvetett anyagi kár több mint 100 emberévvel helyreállítható
- társadalmi-politikai hatás: súlyos bizalomvesztés a Társaság felső vezetésén belül több személyre kiterjedő személyi konzekvenciákkal
- nagy jelentőségű (kiemelt) államtitok sérül

b) A potenciális fenyegető tényező bekövetkezésének gyakorisági osztályát a következők szerint kell meghatározni:

1: nagyon ritka: évente 1-nél is ritkábban
2: ritka: előzőnél gyakrabban, de évente legfeljebb 1 alkalommal,
3: közepes: előzőnél gyakrabban, de évente legfeljebb 12 alkalommal,
4: gyakori: előzőnél gyakrabban, de évente legfeljebb 52 alkalommal,
5: nagyon gyakori: előzőnél gyakrabban, de évente legfeljebb 365 alkalommal
6: különösen gyakori: naponta több alkalommal jelentkezik.

c) A kockázati mátrix kitöltése

Egy adott fenyegetettségre a fentiek szerint megállapított két osztályt (pl. 3 és 5) össze kell adni, a kapott érték az arra a fenyegetettségre jellemző kockázat (a példában K=8), ami dimenzió nélküli mérőszám. A fenyegető tényezőt ezután el kell helyezni a kockázati mátrixon.

A mátrixban három területet határolunk el, például K értéke szerint 2-től 4-ig „alap”, 5-től 9-ig „fokozott”, 10-től 12-ig pedig „kiemelt” fokozatú a kockázat. A tól-ig határokat az üzleti tulajdonos szabadon választhatja meg, szűkebbre vagy bővebbre szabva ezáltal az egyes sávokat. A határoktól függően az egyes kockázati osztályokba kevesebb vagy több elem fog tartozni. A példában K=8, ezért a vizsgált kockázat a középső (a fokozott) sávba tartozik.

		jelentéktelen	kisebb	nagyobb	jelentős	különösen nagy	különösen jelentős
		1	2	3	4	5	6
különösen gyakori	6	7	8	9	10	11	12
nagyon gyakori	5	6	7	8	9	10	11
gyakori	4	5	6	7	8	9	10
közepes	3	4	5	6	7	8	9
ritka	2	3	4	5	6	7	8
nagyon ritka	1	2	3	4	5	6	7

Ezt követően az üzleti tulajdonos dönt a kockázatok elleni védekezésről. Például az alap fokozatúak ellen nem védekezik, és maradó kockázatnak tekinti őket, megemeli vagy éppen csökkenti a sávhatárok értékét és ezzel átsorol néhány elemet az alap fokozatból a kiemeltbe, esetleg éppen fordítva cselekszik. Úgy kell döntéseit meghoznia, hogy a rendszer biztonsága végül megfeleljen kívánalmainak, a szabályzatok előírásainak, de szinkronban legyen erre fordítható anyagi, személyi, stb. erőforrásaival is.

3. sz. melléklet

Informatikai biztonsági nyilatkozat

1. Alulírott kijelentem, hogy a MÁV-START Zrt. számítógépeinek és számítógépes programjainak használatára vonatkozó informatikai biztonsági szabályokat az IBSZ 1. sz. melléklet **Felhasználók biztonsági kötelezettségei** c. segédlet alapján megismertem.

2. Tudomásul veszem, hogy a munkaköröm ellátásához kapott, a MÁV-START Zrt. tulajdonát képező számítógépet (PC, laptop, szoftver, stb.) kizárólag a munkámmal összefüggő feladatok ellátására használhatom, amit a Társaság esetenként ellenőriz.

3. Tudomásul veszem, hogy az általam a számítástechnikai rendszerek és adatok nem előírásszerű használatával és a rendszerek védelmét biztosító technikai intézkedések kijátszásával elkövetett cselekményekért munkajogi, a törvénybe ütköző súlyosságú esetekben pedig büntetőjogi felelősséggel tartozom.

Kelt……..., 20. ……

aláírás: ……..

név: ……

munkakör. ……

készült: 2 példányban
kapják:
1. sz. példány: munkavállaló
2. sz. példány: Humán

4. sz. melléklet

Informatikai fejlesztés biztonsági feladatai és dokumentumai

a) projektindítás

projektlépés		biztonsági tervezés	termék, dokumentum
1.	projekt alapító okirat hatályba lépése		**Projekt alapító okirat** vagy **Rendszerkoncepció** alapvető informatikai biztonsági követelményekkel
2.	projekt- (fejlesztésért felelős) szervezet felállítása		Informatikai biztonsági alteam / alprojekt létrehozása az információvédelmi szakterület munkatársaiból
3.	üzleti tulajdonos kijelölése		
4.	projekt tervezés	informatikai biztonsági feladatok nagybani tervezése, megvalósítási ütemezéssel	**Projektterv**, benne a projekt informatikai biztonsági megfelelőségi rendszerének nagybani meghatározása
5.	az informatikai biztonság kialakítása ütemének tervezése	projektlépések és felelősök megnevezése, határidők hozzárendelése	**informatikai biztonsági alprojekt terve**

b) kockázatelemzés

projektlépés		biztonsági tervezés	termék, dokumentum
1.	biztonsági funkciók tervezése, elfogadtatása	a szállítandó szoftver és a biztonsági termékek biztonsági funkcióinak felmérése, összefoglalása	biztonsági követelmények összefoglalásának ellenjegyeztetése a beszállítóval
2.	kockázatfelmérés és kockázatkezelés	- védendő rendszerelemek azonosítása - fenyegető tényezők azonosítása - fenyegetettség-elemzés - kockázatkezelés	**Kockázatelemzés** c. dokumentum. Tartalma: a rendszer, valamint a fizikai és személyi környezet elemeinek felmérése, a releváns fenyegetések, gyenge pontok feltárása, a nem elviselhető, az elviselhető, és a maradó kockázatok meghatározása, védelmi javaslatok felsorolása, végkövetkeztetésként a rendszer biztonsági osztálya.
3.	biztonsági osztály meghatározása	a rendszerben kezelendő adatok érzékenységének elemzése, titokvédelmi besorolása, kockázatelemzés alapján biztonsági osztályba sorolás (alap, fokozott, vagy kiemelt)	

c) a rendszer biztonságának tervezése

projektlépés		biztonsági tervezés	termék, dokumentum
1.	feladat részleteinek behatárolása	A fizikai, logikai és adminisztratív védelmi rendszer és funkcióinak behatárolása a projekt-dokumentumok felülvizsgálata alapján	**Felülvizsgálati jelentés**
2.	megvalósítási követelményrendszer kidolgozása	informatikai biztonsági követelmények meghatározása az osztályba sorolás alapján	**Rendszerterv informatikai biztonsági fejezete**
3.	biztonsági tesztelés tervezése	a szállítandó szoftver és biztonsági termékek biztonsági funkciói tesztelésének összefoglalása	**Biztonsági tesztelési terv**
4.	változáskezelés tervezése	A szoftver (modulok) módosítása és verzióváltása szabályainak kialakítása	**Változáskezelési Eljárásrend**
5.	részletes biztonsági szabályok kialakítása	a központi informatikai biztonsági szabályozás alapján a rendszerspecifikus szabályok dokumentumba foglalása	**Rendszerszintű Informatikai Biztonsági Szabályzat** (12. sz. melléklet
6.	Informatikai működésfolytonosság tervezése	a rendszer lehető legkevesebb üzemkieséssel járó működésének megtervezése, felelőseinek megnevezése	**Informatikai Működésfolytonossági Terv**

d) a rendszer használatba vétele

projektlépés		biztonsági tervezés	termék, dokumentum
1.	tesztelés végrehajtása	a megvalósított informatikai rendszer biztonságának felmérése, minősítése, az informatikai rendszerhez kapcsolódó fizikai logikai és adminisztratív védelmi rendszer értékelése	- biztonsági tesztelési jegyzőkönyvek - üzleti tulajdonos nyilatkozata a biztonsági megfelelőségről, a rendszer használatba vételéről
2.	fejlesztés lezárása, a rendszer indítása	a Biztonsági Rendszertervben előírt kezelési, üzemeltetési dokumentumok terítése	

5. sz. melléklet

Kockázatelemzés és kockázatkezelés

I. szakasz: A védelmi igény feltárása

1. lépés: A feldolgozandó adatok feltérképezése

1. feladat: Az informatika-alkalmazás output igényének feltérképezése.
2. feladat: Esetleges különleges szolgáltatások feltérképezése.
3. feladat: Az informatikai rendszerben feldolgozásra kerülő valamennyi adat feltérképezése.

2. lépés: Az informatika-alkalmazás és a feldolgozandó adatok értékének meghatározása

1. feladat: Védelmi igény megfogalmazása.
2. feladat: Hatrészes értékskála rögzítése.
3. feladat: Az értékek hozzárendelése az informatika-alkalmazáshoz és az adatokhoz.

II. szakasz: Fenyegetettség-elemzés

3. lépés: A fenyegetett rendszerelemek feltérképezése

1. feladat: A rendszerelemek feltérképezése.
2. feladat: A rendszerelemek kölcsönös függőségeinek leírása.

4. lépés: Az alapfenyegetettség meghatározása

1. feladat: A fenyegető tényezők és a rendszerelemek összerendelése.
2. feladat: Az összerendelések dokumentálása.

5. lépés: A fenyegető tényezők meghatározása

1. feladat: Az informatikai rendszer gyenge pontjainak feltérképezése.
2. feladat: A fenyegető tényezők meghatározása.

III. szakasz: Elemzés kárérték és gyakoriság szerint

6. lépés: A potenciális károk értékének meghatározása

A kárértékek meghatározásánál az alábbi szempontokat kell figyelembe venni.

- Dologi károk, amelyeknek közvetlen vagy közvetett költségvonzatuk van. Ilyenek lehetnek a infrastruktúra károk, informatikai rendszer elemeinek sérülése, helyreállítási költség.
- Károk a politika és társadalom területén. Ilyenek lehetnek az állami és szolgálati titok megsértése, személyhez fűződő jogok, személyek, csoportok hírnevének károsodása, érzékeny adatok nyilvánosságra kerülése, hamis adatok nyilvánosságra kerülése, közérdekű adatok titokban tartása, bizalomvesztés.
- Gazdasági károk. Ilyenek lehetnek a pénzügyi károk, lopáskárok, cég arculatának romlása, rossz üzleti döntés.
- Személyi biztonság sérülése a felhasználói és üzemeltetői személyzetben.
- Jogszabályok, utasítások megsértése.

1. feladat: Az értékek átvitele a rendszerelemekre.
2. feladat: A károk áttekintő ábrázolása.

7. lépés: A potenciális károk gyakoriságának meghatározása

1. feladat: A gyakorisági skála rögzítése.
2. feladat: A gyakorisági értékek hozzárendelése a fenyegető tényezőkhöz.

IV. szakasz: Kockázatelemzés

8. lépés: A fennálló kockázatok meghatározása és leírása mátrixban

1. feladat: Valamennyi kockázat összeállítása egy áttekintésben.
2. feladat: A kockázati mátrix belső határainak (alap - fokozott - kiemelt) kijelölése

V. szakasz: Kockázat-menedzselés

9. lépés: Az intézkedések kiválasztása

1. feladat: Döntés az egyes fokozatok védelmi szükségletéről.
2. feladat: Az intézkedések kiválasztása.

10. lépés: Az intézkedések értékelése

1. feladat: Az intézkedésekkel leküzdött valamennyi fenyegető tényező feltérképezése.
2. feladat: Az intézkedések kölcsönhatásának leírása.
3. feladat: Az üzemmenetre való kihatások vizsgálata.
4. feladat: Vizsgálat az előírásokkal való egyezésre vonatkozóan.
5. feladat: Az intézkedések hatékonyságának értékelése.

11. lépés: A költség/haszon arány elemzése

1. feladat: Az intézkedések költségeinek megállapítása.
2. feladat: Szükség esetén visszalépés a 9.2 pontba.

12. lépés: A maradványkockázat elemzése

1. feladat: A hatékonysági értékek bedolgozása a kockázat áttekintésbe
2. feladat: A maradványkockázat elemzése.

6. sz. melléklet

Informatikai biztonsági rendszerterv vázlata

1. Az Informatikai biztonsági rendszerterv /informatikai biztonsági fejezet célja
- szükségessége (megalapozza az Informatikai Működésfolytonossági Tervet és a Rendszerszintű Informatikai Biztonsági Szabályzatot, vázlatosan felsorolva, hogy annak a dokumentumnak konkrétan milyen elemekkel kell foglakoznia)
- helye a rendszerben
- áttekintés (ami a rendszertervben eddig tervezve volt, változások visszacsatolása)

2. Fogalomtár (csak az IBSZ fogalmain kívüli meghatározások)

3. Rendszerkörnyezet
Szerep és felelősségi körök (ábrával, leírással)
- üzleti tulajdonos (beosztás megnevezése, feladatai, jogköre)
- vezetők munkakörei (megnevezésük, feladataik, jogkörük)
- felhasználók munkakörei (megnevezésük, feladataik, jogkörük)
- informatikai szolgáltatók (üzemeltető, karbantartó stb., külső fél esetében ISO minőségbiztosítási tanúsítvány, IBSZ megléte)

Rendszer architektúra bemutatása (csak önálló informatikai rendszerterv esetén)

4. Informatikai biztonsággal szemben támasztott követelmények (Csak akkor szükséges a 4. pont, ha nem készült önálló Kockázatelemzés)

4.1 Adatok minősítése
- bizalmasság (bemutatása input / output elemenként és származtatott adatokra, üzleti, szolgálati, államtitok vonatkozásban)
- sértetlenség (bemutatása input / output elemenként)
- rendelkezésre állás (idő és térbeliség bemutatása)

4.2. Értékelés, biztonsági osztály meghatározása
(kockázatelemzés rövid összefoglalása, és az ebből meghatározott biztonsági osztály rögzítése)

5. Informatikai biztonsági rendszer kialakítása (**minden elem a 4. pontban leírtaktól, vagy a Kockázatelemzéstől függ)**

5.1 Adminisztratív védelem
- szabályzatok, dokumentumok kidolgozása,
- azonosítások, hitelesítési mechanizmusok,
- naplózás, annak elemzése (operációs rendszer, felhasználó rendszer, egyéb dobozos rendszerek naplózási eljárásai).

5.2 Fizikai védelem
- helyiségek (épületek, szerverszoba) védelme (víz, villám, tűz, belépés),
- hardver / szoftver védelme (dokumentumokkal történő igazolások- jogtisztaság),
- adathordozók védelme (másolatok, archiválás, adatmentés),
- hálózatok elemeinek védelme (jogosultság, elérhetőség),
- áramellátás feltételei,
- kábelezés biztonsága,
- eszközvédelem (asztali és hordozható PC, hordozható eszközök).

5.3 Logikai védelem
- azonosítok, jelszavak, jelszópolitika,
- hozzáférés-védelem, szerepköri modell ,
- operációs rendszer sajátosságai, védelmi funkciói,
- dobozos termékek sajátosságai védelmi funkciói,
- hálózati védelmek (tűzfal, proxy, DMZ, IP cím beállítások),
- vírusvédelem, adatlopás (adatvesztés) elleni védelem (DLP),
- hordozható eszközök védelme (vírusvédelem, tűzfal),
- titkosítások.

5.4 Személyi feltételek
- oktatások, kiválasztás,
- biztonsági tudat fenntartása,
- ellenőrzések, szankciók.

5.5 Vagyonvédelem
- fizikai vedelem kiterjesztése,
- élőerős védelem.

6. Biztonsági tesztelések értékelése, áttekintése (rendszertervhez igazodva)
- ki, mikor, milyen feltételekkel tesztel,
- sikeresség feltételei,
- rendszer megfelelőségi feltételei,
- biztonsági okmányok megfelelősége, a rendszer átvételének feltételei.

(A 7. és 8 pontot nem minősített rendszerek esetén kell vázlatosan kidolgozni)

7. Változáskezelés megoldása
- változtatási igények kezelése, nyilvántartása
- új elemek kidolgozása
- új elemek rendszerbe illesztése
- változások átvezetése, dokumentálása

8. Informatikai működésfolytonosság tervezésének vázlata
- célja, lényege
- helyzetfeltárás, veszélygócok elemzése
- üzemzavar, működési hiba esetén teendők intézkedések, feladatok
- katasztrófa esetén teendők intézkedések, feladatok

7. sz. melléklet

Minősített biztonsági osztályok követelményei

BIZTONSÁGI OSZTÁLYOK KÖVETELMÉNYEI AZ INFORMÁCIÓBIZTONSÁG SZEMPONTJÁBÓL	
Személyi biztonság	
Fokozott	**Kiemelt**
• A rendszergazdai munkakörökbe, továbbá a munkavégzésre felvett munkavállalók (kulcsfelhasználók) biztonsági alkalmasságát előzetesen meg kell vizsgálni. • A titokbirtokos feladatait a titokká minősített adatok kezelésében, valamint az üzemeltetési feladatokat felelősség szerint szabályozni kell.	Fokozottal megegyezik.
Fizikai és környezeti biztonság	
Fokozott	**Kiemelt**
• A rendszerhez tartozó munkaállomásokat és tartozékaikat, úgy kell elhelyezni, hogy az azokkal kezelt adatok illetéktelenek számára ne legyenek hozzáférhetők (billentyűzetről jelszavak leolvasása, monitoron megjelenő, nyomtatóból kijövő listákba, dokumentumokba betekintés, stb.). • A berendezések karbantartásával kapcsolatos eseményeket, feljegyzéseket rögzíteni kell. A javítási munkát csak a Társaság ezzel megbízott munkavállalójának folyamatos személyes felügyelete mellett lehet végezni. • Az informatikai rendszer elemeit a használatból történő kivonás után is megkülönböztetett figyelemmel kell kezelni. A berendezések üzemen kívül helyezésével kapcsolatos eseményeket rögzíteni kell. • Az adathordozók feleslegessé válása esetén azok más célra történő felhasználása előtt – a minősítő jelzést tartalmazó címke eltávolításával egy időben – olyan törlési eljárást kell alkalmazni, amely garantálja, hogy érzékeny adat nem marad az adathordozón.	• A berendezéseket csak olyan helyiségben szabad üzemeltetni, ahol mind a vezetett, mind a sugárzott elektromágneses tér árnyékolásával az információ kiszivárgása megakadályozható. • A berendezések karbantartása során a felügyeletet az információvédelmi szakterület bevonásával kell biztosítani.

Számítógépes és hálózati szolgáltatások és az üzemeltetés biztonsági szabályai	
Fokozott	**Kiemelt**
• Adatkommunikációs folyamat csak a kommunikációban résztvevő felek kölcsönös azonosítása és hitelesítése után kezdeményezhető. • Amennyiben személyes, vagy üzleti titkot képező adatokat nyomtatásban vagy képernyőn megjelenítik, akkor kötelezően fel kell tüntetni előbbiben a „Nem nyilvános” kezelési jelzést, utóbbiban a minősítési jelzést és a titokvédelmi szabályzatokban előírt alaki kellékeket.	Fokozottal megegyezik.
Hozzáférés menedzsment	
Fokozott	**Kiemelt**
• A rendszert futtató PC-ken kötelező a jelszavas képernyővédőt bekapcsolni, ha azt a kezelő ideiglenesen magára hagyja.	Fokozottal megegyezik.

BIZTONSÁGI OSZTÁLYOK KÖVETELMÉNYEI A RENDELKEZÉSRE ÁLLÁS SZEMPONTJÁBÓL	
Fizikai és környezeti biztonság	
Fokozott	**Kiemelt**
• A rendszerekhez hardver karbantartási szerződést kell kötni, ami tartalmazza a megelőző karbantartások módját, a javító karbantartás igénye esetén a maximális reakcióidőt, javítási időtartamot, elhúzódó javítás idejére tartalék eszközök biztosítását.	• A berendezésekhez helyi áramfejlesztőt kell telepíteni, amely a betáplálás tartós hiánya esetén biztosítja a szükséges villanyáramot. A tartalék generátorokat – a gyártó specifikációja szerint – rendszeresen tesztelni, az üzemanyag előírt mennyiségét ellenőrizni kell.

Számítógépes és hálózati szolgáltatások és az üzemeltetés biztonsági szabályai	
Fokozott	**Kiemelt**
• Az informatikai rendszer (vagy annak bármely eleme) dokumentációját a változáskezelés keretében kell aktualizálni és naprakészen tartani. • Az információs rendszer, alkalmazói programok és rendszerleíró paraméterek, rendszerszoftver- és hardver, továbbá hálózati eszközök és rendszerelemek változtatásait ellenőrzött és dokumentált módon kell elvégezni. • A rendszer biztonsági beállításainak megváltoztatása csak dokumentáltan és az információvédelmi szakterület tájékoztatásával történhet. • Adathordozók tárolása csak megbízhatóan zárt helyiségben, minimum 30 perces tűzállóságú tároló szekrényben történhet.	• Adathordozók tárolása csak minimum 60 perces tűzállóságú tároló szekrényben történhet.

8. sz. melléklet

Biztonsági tesztelési jegyzőkönyv

1. A teszt célja:			
2. A tesztelés helye, időpontja:			
3. A tesztelést végezte:			
A tesztelendő programok / modul(ok) azonosítása			
4. Rendszer:		**4. Teszt jellege**: (biztonsági	
5. Alrendszer:		**6. Modul(ok):**	
7. Program / dialógus/ riport:		**8. Verziószám:**	
9. A tesztelés hardver és szoftver környezete:			
10. A teszt input adatai (helye, mennyisége, felvételi módja stb)**:**			
11. A teszt végrehajtása:			
12. A tesztelés eredménye (outputok leírása, tapasztalt rendellenesség leírása, értékelés stb):			
13. Szükséges intézkedések:			
14. Megjegyzés:			
a teszt eredményének elfogadása / jóváhagyása			
kivitelező részéről:		**üzleti tulajdonos / megbízottja(i):**	
név, aláírás		név, aláírás	
dátum		dátum	
név, aláírás		név, aláírás	
dátum		dátum	

A jegyzőkönyvet átvette:

üzleti tulajdonos: ……. **dátum: ……..**

9. sz. melléklet:

IT Működésfolytonossági Terv vázlata

1. Bevezetés
- 1.1. Célja
- 1.2. Hatálya
  - a) személyi hatálya
  - b) tárgyi hatály
  - c) területi hatály
- 1.3. A terv karbantartásáért felelős

2. Fogalmak, rövidítések (ha szükséges)

3. Rendszer és környezet
- 3.1. Biztonsági osztály
  - a) információvédelmi szempontból (elemei: bizalmasság, sértetlenség)
  - b) a rendelkezésre állási követelmények alapján
- 3.2. A rendszer fizikai és működési környezetének bemutatása
  - a) fizikai kiépítettség
  - b) tűzvédelem
  - c) szerverszoba belépés
  - d) áramellátás
- 3.3. felhasználók
- 3.4. A támogatott üzleti folyamat bemutatása
  - a) érzékenység meghatározása
  - b) elviselhető kiesési idő meghatározása

4. Általános és megelőző intézkedések
- 4.1. Kommunikáció
- 4.2. Szolgáltatók
- 4.3. Munkatársak
- 4.4. Dokumentumok módosítása, tárolása
- 4.5. Fizikai infrastruktúra
- 4.6. Adathordozók védelme
- 4.7. Tesztelési eljárások
- 4.8. Oktatás, gyakorlás

5. Személyi feltételek
- 5.1. Működésfolytonossági menedzsment szervezete
- 5.2. Működésfolytonossági menedzsment feladatai

6. Rendkívüli események bekövetkezésekor szükséges intézkedések
- 6.1. Rendkívüli esemény meghatározása, kategorizálása
- 6.2. Rendkívüli esemény bekövetkezése
- 6.3. Munkatársak feladatai
  - a) Működésfolytonossági vezető feladatai
  - b) Üzleti tulajdonos feladatai
  - c) Vezető feladatai
  - d) Rendszergazda feladatai
  - e) Technikai üzemeltető feladatai
  - f) Hálózatfelügyelet feladatai
  - g) Általános munkavállalói feladatok

6.4. Katasztrófahelyzet esetében a teendők
- a) Értesítés menete
- b) Fizikai védelmi kötelezettség
- c) Rendszer helyreállítása
- d) Rendszer visszaállítása
- e) Rendszer áttelepítése
- f) Eszközök ismételt üzembe helyezése
- g) Tartalék eszközök igénybevételének rendje, módja
- h) Kiesett IT munkafolyamatokat helyettesítő eljárások beindítása
- i) adminisztrációs és dokumentálási kötelezettség

7. Eseményelemzés, karbantartás, módosítás, javaslatok

7.1. Események elemzése

7.2. IT Működésfolytonossági Terv karbantartása

10. sz. melléklet

Az IBSZ tartalmát meghatározó vagy befolyásoló jogforrások

a) 2012. évi C. tv. a Büntető Törvénykönyvről rendelkezései közül különösen:
- 219. §: személyes adattal visszaélés,
- 220. §: közérdekű adattal visszaélés,
- 223. §: magántitok megsértése,
- 224. §: levéltitok megsértése,
- 375. §: információs rendszer felhasználásával elkövetett csalás,
- 384. §: bitorlás,
- 385. §: szerzői vagy szerzői joghoz kapcsolódó jogok megsértése,
- 386. §: védelmet biztosító műszaki intézkedés kijátszása,
- 413. §: gazdasági titok megsértése,
- 418. §: üzleti titok megsértése,
- 422. §: tiltott adatszerzés,
- 423. §: információs rendszer vagy adat megsértése,
- 424. §: információs rendszer védelmét biztosító technikai intézkedés kijátszása,
- 459. §: az érték, a kár, valamint a vagyoni hátrány.

b) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

c) 1999. évi LXXVI. tv. a szerzői jogról:
- VI. fejezet: számítógépi programalkotás (szoftver),
- VII. fejezet: adatbázis

MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények. c. szabvány

MSZ ISO/IEC 27002:2007 - Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve. c. szabvány

d) MSZ ISO / IEC 15408 Common Criteria (Az informatikai biztonságértékelés közös szempontjai),

e) MeH Informatikai Tárcaközi Bizottság:
- 8. sz. ajánlás: Informatikai biztonsági módszertani kézikönyv
- 12. sz. ajánlás: Informatikai rendszerek biztonsági követelményei
- 15. sz. ajánlás: Infrastruktúra menedzsment

f) 103/2003. (XII.27.) GKM. r. (Országos Vasúti Szabályzat): B 3.3 fejezet Vasúti informatika,

g) MeH Informatikai Tárcaközi Bizottság:
- 8. sz. ajánlás: Informatikai biztonsági módszertani kézikönyv
- 12. sz. ajánlás: Informatikai rendszerek biztonsági követelményei
- 15. sz. ajánlás: Infrastruktúra menedzsment

h) 103/2003. (XII.27.) GKM. r. (Országos Vasúti Szabályzat): B 3.3 fejezet Vasúti informatika,

11. sz. melléklet

Számítástechnikai bűncselekmények a Büntető Törvénykönyvben
(A jogszabály 2013. november 6-án hatályos állapotának megfelelő szövegét tartalmazza.)

a) 2012. évi C. törvény a Büntető Törvénykönyvről

XXI. FEJEZET

AZ EMBERI MÉLTÓSÁG ÉS EGYES ALAPVETŐ JOGOK ELLENI BŰNCSELEKMÉNYEK

...

Személyes adattal visszaélés

219. § (1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy

b) az adatok biztonságát szolgáló intézkedést elmulasztja,

vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.

(3) A büntetés két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges adatra követik el.

(4) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.

Közérdekű adattal visszaélés

220. § (1) Aki a közérdekű adatok nyilvánosságáról szóló törvényi rendelkezések megszegésével

a) közérdekű adatot az adatigénylő elől eltitkol, vagy azt követően, hogy a bíróság jogerősen a közérdekű adat közlésére kötelezte, tájékoztatási kötelezettségének nem tesz eleget,

b) közérdekű adatot hozzáférhetetlenné tesz vagy meghamisít, illetve

c) hamis vagy hamisított közérdekű adatot hozzáférhetővé vagy közzé tesz,

vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a közérdekű adattal visszaélést jogtalan haszonszerzés végett követik el.

...

Magántitok megsértése

223. § (1) Aki a foglalkozásánál vagy közmegbízatásánál fogva tudomására jutott magántitkot alapos ok nélkül felfedi, vétség miatt elzárással büntetendő.

(2) A büntetés egy évig terjedő szabadságvesztés, ha a bűncselekmény jelentős érdeksérelmet okoz.

Levéltitok megsértése

224. § (1) Aki

a) másnak közlést tartalmazó zárt küldeményét megsemmisíti, a tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja, illetve

b) elektronikus hírközlő hálózat útján másnak továbbított közleményt kifürkész,

ha súlyosabb bűncselekmény nem valósul meg, vétség miatt elzárással büntetendő.

(2) A büntetés egy évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekményt foglalkozás vagy közmegbízatás felhasználásával követik el.

(3) A büntetés

a) két évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekmény,

b) bűntett miatt három évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény

jelentős érdeksérelmet okoz.

XXXVI. FEJEZET

A VAGYON ELLENI BŰNCSELEKMÉNYEK

...

Információs rendszer felhasználásával elkövetett csalás

375. § (1) Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás jelentős kárt okoz, vagy

b) a nagyobb kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás különösen nagy kárt okoz, vagy

b) a jelentős kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(4) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás különösen jelentős kárt okoz, vagy

b) a különösen nagy kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(5) Az (1)-(4) bekezdés szerint büntetendő, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt.

(6) Az (5) bekezdés alkalmazásában a külföldön kibocsátott elektronikus készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül.

XXXVII. FEJEZET

A SZELLEMI TULAJDONJOG ELLENI BŰNCSELEKMÉNYEK

Bitorlás

384. § (1) Aki

a) más szellemi alkotását sajátjaként tünteti fel, és ezzel a jogosultnak vagyoni hátrányt okoz,

b) gazdálkodó szervezetnél betöltött munkakörével, tisztségével, tagságával visszaélve más szellemi alkotásának hasznosítását vagy az alkotáshoz fűződő jogok érvényesítését attól teszi függővé, hogy annak díjából, illetve az abból származó haszonból vagy nyereségből részesítsék, illetve jogosultként tüntessék fel,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(2) E § alkalmazásában szellemi alkotás:

a) a szerzői jogi védelem alá tartozó irodalmi, tudományos vagy művészeti alkotás,

b) a szabadalmazható találmány,

c) az oltalmazható növényfajta,

d) az oltalmazható használati minta,

e) az oltalmazható formatervezési minta,

f) a mikroelektronikai félvezető termék oltalmazható topográfiája.

Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése

385. § (1) Aki másnak vagy másoknak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát vagy jogait vagyoni hátrányt okozva megsérti, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki a szerzői jogról szóló törvény szerint a magáncélú másolásra tekintettel a szerzőt, illetve a kapcsolódó jogi jogosultat megillető üreshordozó díj, illetve reprográfiai díj megfizetését elmulasztja.

(3) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a szerzői vagy szerzői joghoz kapcsolódó jogok megsértését nagyobb vagyoni hátrányt okozva követik el.

(4) Ha a szerzői vagy szerzői joghoz kapcsolódó jogok megsértését

a) jelentős vagyoni hátrányt okozva követik el, a büntetés bűntett miatt egy évtől öt évig,

b) különösen nagy vagyoni hátrányt okozva követik el, a büntetés két évtől nyolc évig,

c) különösen jelentős vagyoni hátrányt okozva követik el, a büntetés öt évtől tíz évig

terjedő szabadságvesztés.

(5) Nem valósítja meg az (1) bekezdés szerinti bűncselekményt, aki másnak vagy másoknak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát vagy jogait többszörözéssel vagy lehívásra történő hozzáférhetővé tétellel sérti meg, feltéve, hogy a cselekmény jövedelemszerzés célját közvetve sem szolgálja.

Védelmet biztosító műszaki intézkedés kijátszása

386. § (1) Aki a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedést haszonszerzés végett megkerüli, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedés megkerülése céljából

a) az ehhez szükséges eszközt, terméket, számítástechnikai programot, berendezést vagy felszerelést készít, előállít, átad, hozzáférhetővé tesz, vagy forgalomba hoz,

b) az ehhez szükséges vagy ezt könnyítő gazdasági, műszaki vagy szervezési ismeretet másnak a rendelkezésére bocsátja.

(3) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a műszaki intézkedés kijátszását üzletszerűen követik el.

(4) Nem büntethető a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedés megkerüléséhez szükséges eszköz, termék, berendezés, felszerelés készítése vagy előállítása miatt az, aki mielőtt tevékenysége a hatóság tudomására jutott volna, azt a hatóság előtt felfedi, és az elkészített, illetve az előállított dolgot a hatóságnak átadja, és lehetővé teszi a készítésben vagy az előállításban részt vevő más személy kilétének megállapítását.

XLI. FEJEZET

A GAZDÁLKODÁS RENDJÉT SÉRTŐ BŰNCSELEKMÉNYEK

Gazdasági titok megsértése

413. § (1) Az a bank-, értékpapír-, pénztár-, biztosítási vagy foglalkoztatói nyugdíjtitok megtartására köteles személy, aki bank-, értékpapír-, pénztár-, biztosítási vagy foglalkoztatói nyugdíjtitoknak minősülő adatot jogtalan előnyszerzés végett, vagy másnak vagyoni hátrányt okozva illetéktelen személy részére hozzáférhetővé tesz, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Nem valósítja meg a gazdasági titok megsértését, aki

a) a közérdekű adatok nyilvánosságára és a közérdekből nyilvános adatra vonatkozó törvényben meghatározott kötelezettségének tesz eleget, vagy

b) a pénzmosás és a terrorizmus finanszírozása megelőzésével és megakadályozásával, a bennfentes kereskedelemmel, piacbefolyásolással és a terrorizmus elleni küzdelemmel kapcsolatos, törvényben előírt bejelentési kötelezettségének tesz eleget, vagy ilyet kezdeményez, akkor sem, ha az általa jóhiszeműen tett bejelentés megalapozatlan volt.

XLII. FEJEZET

A FOGYASZTÓK ÉRDEKEIT ÉS A GAZDASÁGI VERSENY TISZTASÁGÁT SÉRTŐ BŰNCSELEKMÉNYEK

Üzleti titok megsértése

418. § Aki jogtalan előnyszerzés végett, vagy másnak vagyoni hátrányt okozva üzleti titkot jogosulatlanul megszerez, felhasznál, más személy részére hozzáférhetővé tesz vagy nyilvánosságra hoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

XLIII. FEJEZET

TILTOTT ADATSZERZÉS ÉS AZ INFORMÁCIÓS RENDSZER ELLENI BŰNCSELEKMÉNYEK

Tiltott adatszerzés

422. § (1) Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

a) más lakását, egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,

b) más lakásában, egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy rögzíti,

c) más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,

d) elektronikus hírközlő hálózat - ideértve az információs rendszert is - útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki fedett nyomozó vagy a bűnüldöző hatósággal, illetve titkosszolgálattal titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából az (1) bekezdésben meghatározottakon kívül információt gyűjt.

(3) Az (1) bekezdés szerint büntetendő, aki az (1)-(2) bekezdésben meghatározott módon megismert személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot továbbít vagy felhasznál.

(4) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha az (1)-(3) bekezdésben meghatározott tiltott adatszerzést

a) hivatalos eljárás színlelésével,

b) üzletszerűen,

c) bűnszövetségben vagy

d) jelentős érdeksérelmet okozva

követik el.

Információs rendszer vagy adat megsértése

423. § (1) Aki

a) információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad,

b) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy

c) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,

vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha az (1) bekezdés *b)-c)* pontjában meghatározott bűncselekmény jelentős számú információs rendszert érint.

(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.

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

Információs rendszer védelmét biztosító technikai intézkedés kijátszása

424. § (1) Aki a 375. vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő

a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve

b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja,

vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Nem büntethető az (1) bekezdés *a)* pontjában meghatározott bűncselekmény elkövetője, ha - mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntető ügyekben eljáró hatóság tudomására jutott volna - tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

(3) E § alkalmazásában jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító.

ZÁRÓ RÉSZ

Értelmező rendelkezések

459. §

...

(6) E törvény alkalmazásában az érték, a kár, valamint a vagyoni hátrány

a) ötvenezer-egy és ötszázezer forint között kisebb,

b) ötszázezer-egy és ötmillió forint között nagyobb,

c) ötmillió-egy és ötvenmillió forint között jelentős,

d) ötvenmillió-egy és ötszázmillió forint között különösen nagy,

e) ötszázmillió forint felett különösen jelentős.

12. sz. melléklet

A Rendszerszintű Informatikai Biztonsági Szabályzat vázlata

1. Bevezetés
   - Rendszerszintű Informatikai Biztonsági Szabályzat célja,
   - A rendszer informatikai biztonsági osztályai (információvédelem, rendelkezésre állás)
   - A szabályzat hatálya
   - Személyi hatálya
   - Tárgyi hatálya
   - A szabályzat érvényessége
   - RIBSZ felülvizsgálati, karbantartási rend
   - Kapcsolódás más szabályzatokhoz
   - a rendszerkörnyezet, architektúra, rendszerkapcsolatok bemutatása
   - oktatási feladatok

2. Fogalom meghatározások

3. Szerep-, és felelősségi körök
   - Irányító, felügyelő szerepkörök
   - Informatikai szolgáltató
   - Hierarchia ábra
   - Üzleti tulajdonos
   - Rendszergazda
   - Szakterületi vezetők
   - Felhasználók
   - Biztonság szervezetének munkatársai

4. Személyi biztonság
   - Munkavállalókkal szemben támasztott általános feltételek
   - Nem a Társaság. munkavállalóival szemben támasztott feltételek
   - Munkavállalói változások
   - Oktatás
   - Munkavállalói kötelezettségek megszegése esetén követendő eljárás

5. Fizikai és környezeti védelem
   - Fizikai biztonsági tartományok
   - Szerverszoba
   - A munkavégzés szabályai a szerverszoba területén
   - Az eszközök elhelyezése és védelme
   - Épületek, helyiségek fizikai jellemzőinek meghatározását
   - Nyílászárokkal szembeni követelményeket
   - Tűzvédelem
   - Vízvédelem
   - Elektronikus zavarvédelem
   - Áramellátás
   - A villámvédelem
   - A kábelezés biztonságos kialakítása
   - Az eszközök karbantartása, karbantartási napló
   - A rendszer és az adatátviteli hálózat eszközeinek védelme
   - Vagyonvédelmi feladatok

6. Kommunikációval és üzemeltetéssel kapcsolatos biztonsági szabályok
   - Üzemeltetési eljárások, rendszerhatárok
   - Dokumentált üzemeltetési eljárások
   - Feladatkörök szétválasztása
   - Üres íróasztal szabály
   - „Tiszta képernyő” szabály
   - Vírusvédelem
   - Adatmentési eljárás ismertetése
   - Mentések ellenőrzése, szerverre visszatöltés
   - Mentések kezelése (tárolás, címkézés, nyilvántartás stb.)
   - Eseménynaplók
   - Üzemeltetési naplók
   - Üzemeltetési naplók elemzése
   - Adatátviteli hálózat
   - Hálózati elemek beállításai
   - Adathordozók kezelése
   - Elektronikus adathordozók kezelése
   - Licencek és PC image kezelés
   - Mentés kezelés
   - Dokumentumok kezelése, tárolása, selejtezése
   - Adathordozók törlése, selejtezése

7. Jogosultság-kezelés
   - Hozzáférési jogosultságok
   - Felhasználók hozzáférés-menedzsmentje
   - Felhasználók azonosítása
   - Authentikáció
   - A privilégiumok kezelése
   - Felhasználói jelszavak
   - A felhasználói jogosultságok áttekintése
   - A felhasználók feladatai
   - Jelszóhasználat
   - A jelszókiválasztás szabályai
   - Rendszer zárolása
   - A hozzáférés-kontroll technikai megvalósítása (távoli bejelentkezés, helyi bejelentkezés)
   - Felhasználó be/kiléptetési folyamata, változások kezelése, jogosultsági űrlap készítése

8. Változáskezelési eljárásrend
   - Változáskezelés
   - Változáskezelés folyamata
   - Karbantartás
   - Dokumentáció kezelés

9. Informatikai működésfolytonosság tervezése
   - célja, lényege
   - helyzetfeltárás, veszélygócok elemzése
   - üzemzavar, működési hiba esetén teendők intézkedések, feladatok
   - katasztrófa esetén teendők intézkedések, feladatok

10. Megfelelősség
   - Hatályban lévő utasítások
   - Biztonsági auditálások, ellenőrzések

13. sz. melléklet

Felhasználó beosztottal rendelkező közvetlen vezető informatikai biztonsági jellegű feladatai

1. Munkavállaló belépése esetén

- Az Informatika szervezeténél megrendeli mindazon informatikai és hordozható eszközöket, melyek szükségesek a munkavégzéshez.
- Megállapítja, hogy a munkatársnak milyen felhasználói rendszerekhez kell hozzáférést biztosítani, és a rendszerekhez tartozó Rendszerszintű Informatikai Biztonsági Szabályzatban szereplő jogosultságkezelési űrlapon a megfelelő kitöltéssel. Ezt az űrlapot mindig az adott rendszer üzleti tulajdonosának, jóváhagyását követően pedig a felhasználói rendszergazdájának kell megküldeni.
- Ha belépő munkavállaló olyan eszközt kap melyen előzőleg már dolgoztak, akkor mérlegelnie kell, hogy az előző munkatárs hivatali dokumentumai szükségesek-e az új munkatársnak. Ha igen, akkor az informatikai szolgáltató által a dokumentumokat át kell másoltatni az új munkatárs profiljába, és az előző munkatárs profilját töröltetnie kell. Ugyanígy kell eljárnia a levelező rendszer használatában is, ahol az előző munkatárs leveleit, beleértve a helyi archív leveleket is át kell tölteni az új munkatárs postafiókjába és archív tárolás helyére.

2. Munkavállaló kilépése esetén

- Kötelezni kell a munkavállalót, hogy a számítógépén, hordozható eszközén, és központi szerveren lévő sajáthasználatú tárterületéről (O: meghajtó) biztonságosan töröljön le minden személyes adatot. A munka anyagok biztonsága érdekében a törlések felügyeletét a közvetlen vezetőnek, vagy megbízottjának kell felügyelnie.
- Kötelezni kell a munkavállalót, hogy a levelező rendszerben is biztonságosan töröljön minden személyes jellegű levelet az aktív és az archív postafiókjából is. A munka anyagok biztonsága érdekében a törlések felügyeletét a közvetlen vezetőnek, vagy megbízottjának kell felügyelnie.
- Kötelezni kell a munkavállalót, hogy az Adatvédelmi Szabályzat 2. számú mellékletét, NYILATKOZAT a magánjellegű és személyes adatok eltávolításról töltse ki, és adja át a közvetlen vezetőnek. Ezt a nyilatkozatot közvetlen vezető a humán ügyintézőnek köteles megküldeni.
- A közvetlen irányítása alá tartozó munkavállaló munkaviszonyának bármilyen okból való megváltozásakor a munkavállaló által az informatikai rendszerekben (pl. DMS-Poszeidon) kezelt adatokhoz, dokumentumokhoz történő további hozzáférésről gondoskodni köteles.
- Az informatikai szolgáltató felé intézkedni kell, hogy a munkatárs informatikai rendszeréhez (AD-ban) való hozzáférési jogát mikortól szüntesse meg.
- Az informatikai szolgáltató felé intézkednie kell, hogy a munkatárs postafiókjára tegyék fel a következő üzenetet: „Tisztelt Levelezőpartnerem! 201x.xx.xx-tól már nem dolgozom a MÁV-START-nál. Munkakörömet XXX veszi át tőlem. Amennyiben levele nem személyes jellegű, akkor kérem, hogy azt ismételten küldje el részére a xxx@mav-start.hu e-mail címre! XXX telefonos elérhetősége: +36 1 51x xxxx. Köszönettel: XXX”. Az üzenetet 30 napig kell fenntartani, azután a postafiókot a tartalmának megtekintés és mentés nélküli törlésével fel kell függeszteni.
- Közvetlen vezetőnek mérlegelnie kell, hogy az eszközt más munkavállaló tovább használja folytatva a kilépő munkáját. Ebben az esetben további törléseket ne végezzen, és új munkatárs esetében járjon el a Munkavállaló belépése pontban leírtak szerint. Amennyiben a kilépő munkatárs adatait már nem fogják tovább használni, intézkedni kell az informatikai szolgáltatónál a munkatárs profiljának a számítógépről történő letörléséről, a munkavállaló által

használt központi adattárolási hely törléséről (O: meghajtó), és az előző bekezdésben meghatározott üzenet használati idejének lejárta után a postafiókjának és archív leveleinek tartalmának megtekintés és mentés nélküli törléséről.

- Ha a munkavállaló kilépésekor a munkakört átvevő személy kiléte még nem ismert és az informatikai eszköz más személy részére kiadásra kerül, akkor az adatok mentéséről és az eszközről történő letörléséről gondoskodni kell. A mentést 2 példányban CD/DVD lemezre kell elkészíteni, vagy az informatikai hálózat szerverére kell felhelyezni. Nagy mennyiségű adatok esetén technikai megoldást jelent egy új, üres merevlemezre történő mentés elkészítése is. A mentés adathordozóit a közvetlen vezető megfelelő biztonsági intézkedés mellett (zárt szekrény, lemezszekrény, páncélszekrény) tárolja.

3. Munkavállaló másik munkakörbe helyezésekor

- Ha a munkavállaló átszervezés során egy másik szervezethez kerül át, de a munkaköre megmarad és az informatikai eszközeit viszi magával további használatra, akkor az általa eddig kezelt adatokat is viszi magával és a rendszerekhez való hozzáféréseket sem kell visszavonni. Ebben az esetben a jelenlegi és az új közvetlen vezető egyeztetésére van szükség.
- Ha a munkavállaló másik munkakörbe kerül át és a munkavégzéshez részére biztosított eszközöket nem használja tovább, akkor a kilépések szerint kell eljárni.
- Ha a munkavállaló másik munkakörbe kerülésekor a munkakört átvevő személy kiléte még nem ismert és az informatikai eszköz más személy részére kiadásra kerül, akkor az adatok mentéséről és az eszközről történő letörléséről gondoskodni kell. A mentést 2 példányban CD/DVD lemezre kell elkészíteni, vagy az informatikai hálózat szerverére kell felhelyezni. Nagy mennyiségű adatok esetén technikai megoldást jelent egy új, üres merevlemezre történő mentés elkészítése is. A mentés adathordozóit a közvetlen vezető megfelelő biztonsági intézkedés mellett (zárt szekrény, lemezszekrény, páncélszekrény) tárolja.

4. Munkavállaló tartós távolléte esetén (Gyes, Gyed, tartós, hosszas betegség, stb.)

- Ha közvetlen vezető úgy ítéli meg, hogy a munkatárs feladatát más fogja átvenni, akkor a 2. Pont szerint kell eljárni, azzal az eltéréssel, hogy a postafiókra a következő üzenetet kell feltenni: „Tisztelt Levelezőpartnerem! 201x.xx.xx-tól hosszabb ideig távol leszek. Munkakörömet XXX veszi át tőlem. Amennyiben levele nem személyes jellegű, akkor kérem, hogy azt ismételten küldje el részére a xxx@mav-start.hu e-mail címre! XXX telefonos elérhetősége: +36 1 51x xxxx. Köszönettel: XXX”. Gondoskodnia kell, hogy a felhasználó AD-ban felfüggesztésre kerüljön. Az üzenetet 30 napig kell fenntartani, azután a postafiókot a tartalmának megtekintés és mentés nélküli törlésével fel kell függeszteni.
- Ha közvetlen vezető úgy ítéli meg, hogy a munkatárs feladatit nem veszi át senki, akkor gondoskodnia kell, hogy a felhasználó AD-ban felfüggesztésre kerüljön, valamint a postafiókja az előző üzenet feltétlét követő 30. napon kerüljön felfüggesztésre.

14. sz. melléklet

Nyilatkozat a maradványkockázatok elfogadásáról
és a rendszer biztonsági osztályba sorolásáról

Alulírott ……., mint a(z) ……... rendszer üzleti tulajdonosa kijelentem, hogy az elkészült kockázatelemzés alapján a ……. rendszert fenyegető tényezőket megismertem, és az „Elviselhető” szintnél magasabb fenyegető tényezők ellen a szükséges intézkedéseket megtettem. Az intézkedésekben meghatározottak teljesülését a rendszer átvételét megelőzően ellenőriztem, és megfelelő megvalósításukról meggyőződtem.

A maradványkockázatok okozta fenyegetettségeket tudomásul veszem, mivel azok az elfogadható szinten és kárértéken belül vannak.

Mindezek alapján a rendszert a következő biztonsági osztályokba sorolom:

Információvédelem szempontjából: …….

Rendelkezésre állás szempontjából: …….

……, 201… …….. hó …… nap

……
üzleti tulajdonos

24/2014. (II. 12. MÁV-START Ért. 9.) sz. vezérigazgatói utasítás a MÁV-START Zrt. Adatvédelmi Szabályzata

1.0 AZ UTASÍTÁS CÉLJA

Az utasítás célja az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) előírásai végrehajtásának szabályozása a MÁV-START Zrt-nél (a továbbiakban: Társaság), különösen a helyi adatkezelések elveinek és rendjének meghatározása, a személyes adatok felhasználási, továbbítási és védelmi szabályainak rögzítése.

2.0. HATÁLY ÉS FELELŐSSÉG MEGHATÁROZÁSA

2.1. Az utasítás hatálya

Az utasítás hatálya a Társaságnál folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira vonatkozik, valamint a Társasággal szerződéses jogviszonyban álló természetes és jogi személyre, jogi személyiséggel nem rendelkező szervezetre, a velük kötött szerződésben, illetve titoktartási nyilatkozatban rögzített mértékben. Az utasítást a számítógéppel, valamint a manuális módon végzett adatkezelésre és adatfeldolgozásra egyaránt alkalmazni kell.

2.2. Az utasítás kidolgozásáért és karbantartásáért felelős

A szabályzat kidolgozásáért és karbantartásáért a Társaság biztonsági vezetője felelős.

3.0. FOGALMAK MEGHATÁROZÁSA

3.1. Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek, vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

3.2. Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

3.3. Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása, megsemmisítése és tönkremenetele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere (a védelem tárgya az adat).

3.4. Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől feltéve hogy a technikai feladatot az adatokon végzik.

3.5. Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – személyes adatok feldolgozását végzi.

3.6. Adathordozó: a papír és azok a számítógépes alkatrészek, eszközök, amelyekre a munkához szükséges adatokat menteni, tárolni lehet, illetve a hordozható változataikkal gép-gép között adatot lehet cserélni, például:

- mágneses elven működő egységek (pl.: FDD, HDD, IBM Microdrive),
- optikai adattárolás elvén működő adathordozók (pl.: CD, DVD, Blu-ray Disc (BD)),
- memóriakártyák (pl.: Smart Media, Compact Flash, SDHC),
- USB, soros, IRDA portra csatlakoztatható eszközök (pl.: pen-drive, okostelefon, fényképezőgép, zenelejátszók, videokamerák).

3.7. Adatkezelés: az alkalmazott eljárástól függetlenül a személyes adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is.

3.8. Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.