1. A szállítandó termék/szolgáltatás

A járművek utasterébe Járműfedélzeti Kamerás Megfigyelő és Rögzítő rendszert (továbbiakban: JKMR) valamint a jármű külső falán lévő Visszapillantó Kamerás rendszert (továbbiakban VK) kell korszerűsíteni valamint karbantartani.

A JKMR és VK rendszerek rendelkezésre állásának meg kell egyeznie a 3. számú mellékletben a járművel szemben meghatározott elvért minimumértékkel.

1.1. Általános leírás

A járművekben korszerűsítendő JKMR rendszernek a járművek belsőtereit kell megfigyelnie, az ott történő eseményeket rögzítenie és a rögzített felvételeket az előírt ideig tárolnia. A járművek külső részén található kamerák a VK rendszer részét képezik és csak visszapillantási funkciójuk van, a kamerák képét tilos rögzíteni. A két rendszer lehet egy központú is, ez esetben a rendszerek közti elhatárolást biztosítani kell. A JKMR rendszer a járműben tartózkodók képmását kezeli és dolgozza fel, ezért meg kell felelnie a 2011. évi CXII. törvény – az információs önrendelkezési jogról és az információszabadságról vonatkozó – rendelkezéseinek. Egyúttal a MÁV-START Zrt. – mint üzembentartó – Informatikai Biztonsági Szabályzata értelmében információvédelmi szempontból a „fokozott" biztonsági osztály követelményeit is ki kell elégítenie.

A JKMR rendszert el kell látni szünetmentes áramforrással, ami a teljes JKMR-rel összefüggő eszközöket képes 24 órán át működtetni, és annak állapotát a saját belső üzemi logjában rögzíteni. Távfelügyeleti rendszer megléte esetén ezeket a jelzéseket legyen képes átjelezni a központ részére.

A korszerűsítendő rendszereknek és részegységeiknek meg kell felelniük az Európai Unió vasúti rendszerének „Járművek – mozdonyok és személyszállító járművek" alrendszerére vonatkozó szerződéskötéskor érvényes 1302/2014/EU (Loc&Pass TSI), 1300/2014/EU (PRM TSI), 1303/2014/EU (SRT TSI) átjárhatósági műszaki előírásoknak.

1.2. Egy motorvonati kamerás rendszer tartalma

A JKMR és VK rendszerből kocsinként egy-egy rendszer kell, mely minimálisan az alábbi egységeket, elemeket tartalmazza:

JKMR rendszer esetén:

- 1 db központ egység (melynek részei a rögzítő egység, a háttértároló, a tápegység, csatoló felületek);
- 8 db vandálbiztos dóm kamera;
- az egység beszereléséhez, üzembe helyezéséhez szükséges speciális szerelési segédanyagok és egyéb alkatrészek (mint pl. video- és egyéb kábelek, csatlakozók és ellendarabjaik, speciális csavarok, csavarzatok);
- Wifi valamint GPRS hálózatot szolgáltató router, hozzá tartozó tetőantennával
- a rendszer üzembe helyezéséhez, üzemeltetéséhez, karbantartásához szükséges szoftverek.

VK rendszer esetén:

- 1 db központ egység (melynek részei a központi egység, a tápegység, csatoló felületek);
- 4 db kültéri vandálbiztos házban szerelt visszapillantó funkciót ellátó kamera;
- 4 db speciális a vezetőállásokon elhelyezett monitorok
- az egység beszereléséhez, üzembe helyezéséhez szükséges speciális szerelési segédanyagok és egyéb alkatrészek (mint pl. video- és egyéb kábelek, csatlakozók és ellendarabjaik, speciális csavarok, csavarzatok);
- a rendszer üzembe helyezéséhez, üzemeltetéséhez, karbantartásához szükséges szoftverek.

A két rendszert lehet üzemeltetni egy központi egységről, ez esetben a külön funkciókat és lehatárolásokat biztosítani szükséges.

A szoftverek esetében a szoftver későbbi fejlesztéséhez szükséges környezetet is át kell adni a szükséges licencekkel, vagy biztosítani kell a szoftver módosítását a Megrendelő igénye alapján az üzembe helyezéstől számított 15 évig.

1.3. JKMR és VK rendszerek elemeinek részletezése

1.3.1. Rögzítő központ

A JKMR központnak alkalmasnak kell lenni egységenként legalább 8 db kamera képének rögzítésére, egy erre alkalmas, a videokamerás megfigyelő és rögzítő rendszer részét képező háttértárolón. VK központnak 4 db kamera és 4 db monitor kezelésére kell képesnek lennie. JKMR rendszer esetében amennyiben a rögzítés merevlemezre történik, akkor ezt hibrid technológiával kell megoldani, aminek a következőképpen kell működnie:

- amíg a környezeti feltételek lehetővé teszik, addig az eszköz merevlemezre rögzít, amennyiben a környezeti feltételek oly mértékben leromlanak, hogy az már a merevlemez normál működését zavarja, vagy az eszközt károsíthatja, a merevlemez kerüljön lekapcsolásra, és a rögzítés kizárólag a félvezetős tárolóra folytatódjon.
- a környezeti feltételek normalizálódásakor a merevlemezre történő rögzítés újból legyen engedélyezve, továbbá a folyamatos rögzítés mellett a korábban kizárólag félvezetős tárolóra mentett képek kerüljenek átmásolásra a merevlemezre.

A rögzítést kameránként legalább 8 kép/másodperc gyakorisággal történjen, ha a kamera által érzékelhető képeken mozgás tapasztalható. A tárhely legkedvezőbb kihasználása érdekében, ha a kamera nem érzékel mozgást, a felvétel rögzítése csökkentett rögzítési gyakorisággal (pl. 1 felvétel/1 másodperc vagy ritkábban) és a legnagyobb tömörítési beállítással történhet. A képek rögzítése analóg rendszer ajánlat esetében minimálisan 960H-s (PAL: 960 x 576; NTSC:960 x 480; továbbiakban: 960H) vagy digitális rendszer ajánlat esetében minimálisan 720P (1280 x 720p, továbbiakban: 720p) felbontásban történjen. A kamerák által biztosított képfelbontás minimum elégítse ki a rögzítő központtal szemben megfogalmazott minimális rögzítési felbontást.

A központ legyen képes rögzíteni a JPEG2000 és a H.264 szabványokat is. A tömörítési beállításoknál minden esetben a HighQuality beállítások alkalmazandóak. Hibrid technológia alkalmazása esetén a félvezetős tárolókat a rögzítővel együtt kell szállítani. A szállítandó

félvezetős tároló méretét úgy kell megválasztani, hogy azon 100%-os mozgást feltételezve az összes kamerát figyelembe véve minimálisan 24 órányi adat tárolására legyen lehetőség. Amennyiben a rögzítő több félvezetős tárolót is képes fogadni, úgy valamennyiben a fenti feltételeknek egyenként eleget tévő méretű félvezetős tárolót kell telepíteni. Bármelyik félvezetős tároló meghibásodása esetén az eszköznek automatikusan képesnek kell lennie a hibás eszközt a működésből kiiktatni és a maradék félvezetős tárolóval képtartalom vesztése nélkül tovább működni.

A rendszernek ellenőrizni kell a saját működését. Amennyiben a rögzítő berendezés működésében valamilyen hiba keletkezik, akkor hibajelzést kell küldenie a jármű központi diagnosztikai rendszerének (a jármű 24 V_{DC} feszültségét kapcsoló alaphelyzetben nyitott kontaktus). A központi rögzítőegységnek a fellépett hibát, eseményt naplóznia kell (esemény jellege, fellépés és megszűnés időpontja). Az eseménynapló tartalmát megfelelő jogosultsághoz kötve kiolvashatóvá kell tenni. A rendszer által generált hibajelzést látható módon a vezetőálláson kialakítandó kiolvasási csatlakozó mellett is meg kell jeleníteni.

A rögzítő egységnek képesnek kell lennie a kamera képébe integrálva megjeleníteni a jármű pályaszámát, a rögzítő jelét („A”, „B”, „C”… betűk egyike), valamint az adott kamera sorszámát, amely összesen minimálisan 8 karakter.

A rögzítő központ belső órájának pontatlansága legfeljebb 1 s lehet 24 óra alatt. A rendszerben biztosítani kell, hogy a téli és nyári időszámításra való átállás automatikusan történjék meg valamennyi eszközön a központilag biztosítandó idő egyidejűségnek megfelelően. A vezérlőegység belső órájának szinkronizálása a GPS berendezés órajelével kell történjen. Üzem közben 4 óránként kell a szinkronizálást elvégeznie.

A készüléknek és a szükséges Informatikai eszközöknek és egyéb tartozékoknak egy 400x450x180 mm-es szekrényben elhelyezhetőnek kell lenni. A szekrényt fizikai hozzáférés ellen biztosítottan minden oldalról zárhatóvá kell tenni oly módon, hogy az eszközök szellőzése biztosítva maradjon. A szekrény ajtaját külön a MÁV-START Zrt. által egyeztetett, csak kódkártyával másoltatható, biztonsági kulcsos szerkezettel kell ellátni.

A videó rögzítő berendezés belső órájának pontos idő szinkronizálásához a járműre telepíteni kell Sencity Rail MIMO 1399.99.0057 típusú antennát. Az előlapra a kiolvasáshoz és szervizcsatlakozáshoz szükséges csatlakozó felületeket ipari kivitelű megoldással kell kivezetni és porvédő kupakkal kell ellátni.

A központi egységet a Szállítónak el kell látnia legalább 2.0-ás USB és legalább 100Mbit/s sebességű Ethernet csatlakozással rendelkező interfészekkel, melyek lehetővé teszik szerviz számítógép csatlakoztatását, amellyel a központ és annak eseménytárolója lekérdezhető, paraméterei megváltoztathatóak, valamint a rögzített képi tartalom kiolvasható. A csatlakozás során a kommunikációnak egyszerűnek, megbízhatónak (hibamentesnek) és dokumentáltnak (naplózottnak) kell lennie. A központi egység előlapján az egyes videobemenetek állapotát (a bemenet nincs használva, hibás rögzítés, rögzítés rendben történik) jeleznie kell.

A korszerűsítéssel együtt ki kell építeni Ethernet hálózatot is, aminek végpontokat kell biztosítson a járműfedélzeti kamerás megfigyelőrendszer központja, valamint a kiolvasások elvégzéséhez valamennyi vezetőálláson, továbbá kapcsolatot kell teremtsen a routerrel is. A hálózatnak a rögzítő egység sebességéhez kell illeszkednie, annál lassabb aktív és passzív rendszerelemek beépítése nem megengedett. A rögzített képek kiolvasását a járművek közlekedése esetén is biztosítani kell. A rögzítő egység kiolvasását valamennyi vezetőálláson el kell tudni végezni.

A JKMR rendszer Ethernet hálózatához MÁV Zrt. Műszaki Felügyeleti és Technológiai Igazgatóság, Technológiai Központ által megadott C819HGW+7-E-K9 típusú router egységet

kell csatlakoztatni, amellyel a MÁV Zrt. helyi WiFi hálózataihoz biztonságosan tudnak a JKMR rendszer rögzítői csatlakozni.

1.3.2. Kamera

Vandálbiztos, színes dóm-kamera, melyek a vasúti járművek belső terében, a mennyezetre lesznek rögzítve. A kameráknak minden napszak idején is megfelelő minőségű képet kell szolgáltatnia. A vasúti üzemi körülményeknek (mechanikai, környezeti és villamos – melyek a megadott szabványokban rögzítettek) meg kell felelnie.

Felbontás:	legalább 960H vagy 720p
Kivitel:	vandálbiztos házba szerelt, Mini DOME kivitelnek megfelelő alakú
Fényérzékenység:	Színes:0,1 lux/F2.0 vagy annál jobb
	Fekete-fehér: 0,01 lux/F2.0 vagy annál jobb
Elektronikus rekesz:	automatikus és 1/100,000-ig állítható
Méret (h x sz x ma):	maximálisan 130 x 130 x 80 mm
További specifikációk:	BLC, HLC, WDR (vagy HDR), AGC
Kamera lencse:	változtatható legalább 3-9mm között

A termes kocsikban kb. 6,5 m hosszúságú és 2,6 m széles területet kell egy kamerának értékelhetően látnia, a kamerák által megfigyelt területen a felbontás mértéke minimum 250 pixel/méter legyen a legtávolabbi ponton, valamint biztosítson arcfelismerést.

Az előterekben maximálisan 2600 x 2600 mm-es területet kell megfigyelni, itt alkalmazható 180°-os látószögű mennyezeti kamera is, amely a le- és felszállás folyamatát mutatja. A felbontási paraméterek itt is elégítsék ki a 250 pixel/méteres értéket.

1.3.3. Háttértároló

Amennyiben hibrid technológiával történik a rögzítés, akkor a merevlemeznek meg kell felelnie a vasúti üzemi körülményeknek (mechanikai, környezeti és villamos – melyek a megadott szabványokban rögzítettek), és alkalmasnak kell lennie a kamerák által biztosított High Quality felbontású (960H vagy 720p), minimum 8/fps rögzítési sebességű, a rögzítőre kötött maximális kameraszám figyelembevételével a képek legalább 30 napon át történő tárolására. A rögzítő rendszer rendelkezzen beépített gyorsulásmérővel a korábban ismertetett hibrid funkció kielégítésére. A rögzítés történhet más típusú adattárolóra is, mely megfelel a vasútüzemi követelményeknek (rázás, ütés, klíma) és rendelkezik a minimálisan szükséges tároló kapacitással például SSD meghajtó.

1.3.4. Adattárolás

A rögzített képet felhasználás hiányában a rögzítéstől számított beállítási időt követően meg kell semmisíteni, törölni kell, a mindenkor hatályos magyar jogszabályok szerint (jelenleg ez az idő 15 nap).

Az adatrögzítőnek a háttértároló kapacitásának határáig a rögzített felvételek HighQuality minőségű és legalább 8 fps sebesség beállítása mellett lehetővé kell tennie, hogy a rögzítési

időintervallum értéke legalább 30 napra kiterjeszthető legyen rendszergazdai joggal bíró személy által.

A rendszernek biztosítani kell a 2011. évi CXII törvény 7. § adatbiztonsági pontjában meghatározottakat:

- A felvett adatokat rejtjelezetten kell tárolni a rögzítő berendezésen, hogy illetéktelen hozzáférés esetén ne legyen megismerhető a rögzített felvétel.
- Arra jogosult hozzáférése esetén biztosítani kell az adatok kimentésének lehetőségét úgy, hogy a felvétel tartalmát a kimentésben közreműködő személy ne ismerhesse meg.
- A rögzített adatok rejtjelezett formátumban kerüljenek kiírásra, majd továbbításra a hatósági felhasználásig.

1.3.5. Adatok kiolvasása és lejátszása

Olyan rendszert kell alkalmazni, amelyben biztosított, hogy a felvételt a kimentésében közreműködő személyek ne ismerhessék meg. A kiolvasásra használt szoftver adjon megfelelő visszajelzést arra vonatkozóan, hogy a kérdéses kiolvasási időintervallumban van-e felvétel vagy sem. Olyan fájlformátumot kell alkalmazni, amely a közismert lejátszó programokkal nem nyitható meg.

A kiolvasás alapvetően nem eredményezheti a rögzített felvételek törlését a merevlemezről csak abban az esetben, ha szelektív törlés történik.

A videó megfigyelő rendszerhez szállítani kell egy kiolvasó és egy lejátszó szoftvert, ami lehetővé teszi, hogy a háttértárolón kódolva tárolt videó kiolvasható és lejátszható legyen. Biztosítani kell, hogy a háttértárolót más számítógépbe áthelyezve – amin nem fut a kiolvasó vagy a lejátszó szoftver – az adatokat ne lehessen kiértékelhető módon megjeleníteni. A kiolvasást a háttértároló kivétele nélkül kell megvalósítani. A kiolvasó szoftver a kiíráskor megadandó paraméterek között adjon lehetőséget arra vonatkozóan, hogy a mentendő file mérete a mindenkori program méretével együtt maximálisan egy DVD méretű legyen, biztosítva ezzel az egy DVD-re rögzíthető maximális méretet, valamint nagyobb méret esetén automatikusan tördelje a megfelelő méretre. Tördelés esetén a tördelt fájlokhoz is generáljon kódot.

A rögzítő központokat egy a jármű egyéb rendszerei által használt számítógépes hálózattól elkülönített számítógépes hálózatba kell szervezni. A hálózathoz olyan routert és antennát kell telepíteni, amivel képes legyen kapcsolatot létesíteni a MÁV Zrt. Műszaki Felügyeleti és Technológiai Igazgatóság, Technológiai Központ által megadott VPN-el védett WiFi-s hálózatához. A MÁV által megadott C819HGW+7-E-K9 típusú routert a Szállítónak kell biztosítania. A kapcsolattal kerül biztosításra a központi felügyelet és a távoli kiolvashatóság a törvényi szabályozások betartása mellett. A központi hálózatnak olyan sebességűnek kell lennie, hogy biztosított legyen a gyors kimentés lehetősége.

A kiolvasási sebességnek minimum 10 MB/s sebességűnek kell lennie, ezt a sebességet duál módban, azaz a kamerák képeinek folyamatos rögzítése mellett a kiolvasásnak egy időben kell tudnia megvalósítania.

A szerviz számítógéppel kiolvasott adatokat a hatóságnak egy erre alkalmas, egyszer írható adathordozón (DVD-n, mely a 27/2014. (II. 12. MÁV-START Ért. 9.) VIG sz. vezérigazgatói utasításnak megfelelő) kell átadni. Az adathordozóra történő mentésre használt, a kiolvasó számítógépre telepítendő szoftvert is biztosítania kell a Szállítónak. A hatóság részére átadott

adathordozón lévő lejátszó program ne tartalmazzon a lejátszáson, kódazonosításon kívül egyéb programrészleteket. A szoftver olyan kialakítású, hogy az adathordozón lévő minden adat – ha azon több járműből vagy kocsi részből származó adatok is rögzítve vannak – csak a megfelelő jelszó megadása után váljon hozzáférhetővé. A megfelelő jelszót a kiolvasó program automatikusan generálja, ami a kiolvasás során nem látható. A programok kialakításánál törekedni kell a lehető legkisebb méretre.

Az adathordozón automatikusan az alábbiakat kell rögzíteni:

- lejátszó program maximálisan 1 példányban
- a felvételek

A kódolt jelszó egy olyan külön segédprogrammal váljon láthatóvá, mely kizárólag a Megrendelőnek kerül átadásra.

A hatóságnak átadott kódolt felvételek a lejátszó programmal, de annak külön telepítése nélkül, a jelszó megadását követően váljanak megtekinthetővé. Az adathordozón lévő lejátszó szoftver csak az adathordozón lévő képanyag megjelenítésére legyen alkalmas.

A rögzítő központhoz tartozó IP cím nem publikus, ezért azt az eszközön feltüntetni nem szabad. A címet a Megrendelővel egyeztetve kell beállítani.

A háttértárolóhoz történő hozzáférést a rendszernek naplóznia kell. A naplóban szerepelnie kell a csatlakozó felhasználó azonosítójának, tevékenységének, valamint a csatlakozás időpontjának. A programnak olyan memóriaréssel is kell rendelkeznie, amelyből visszakereshetőek a felhasználók tevékenységei.

Az utas a 2011. évi CXII törvény 14. § c) pontjában adott jogával élhet és kérheti a személyes képi adatainak törlését. Ehhez olyan technikai megoldást kell a rendszerbe beépíteni, amely biztosítja a fenti típusú szelektív adattörlést. A kiolvasó személy részére ehhez a felvétel kiírása előtt választási lehetőséget kell biztosítani:

- a „kiírás-törlés nélkül”vagy;
- a „kiírás-törléssel”

opciók felajánlásával. Amennyiben a 2. műveletet választja a kiolvasó személy, a kért időtartam rögzített képeinek sikeres kiírását követően a felvételeket a rögzítő egységből automatikusan törölni kell.

A karbantartást végzők számára a működés ellenőrzéséhez a kameraképek valós időben legyenek láthatóak a rendszeridővel együtt.

1.3.6. Javíthatatlan, leselejtezett adathordozó eszközök kezelése

A műszaki, gazdasági okokból nem javítható, valamint a leselejtezett, de még személyes adatokat tartalmazó adathordozó eszközök vonatkozásában a Szállító tételes lista szerint, jegyzőkönyvben rögzített formában a biztonsági kamerarendszert üzemeltető MÁV-START Zrt. információbiztonság szakértője jelenlétében gondoskodik a merevlemezek olyan szintű megsemmisítéséről, hogy az azokon tárolt személyes adatok véglegesen és visszaállíthatatlan módon megsemmisítésre kerüljenek.

1.3.7. Hozzáférési jogosultságok

A felvétel kimentése során a rögzítő egység a számítógéppel automatikusan lépjen kapcsolatba az IP cím megadása után. Ez a kapcsolat legyen felhasználóként eltérő jelszavakkal védve. A rendszerben biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága a szerepkörüknek megfelelő legyen. Ennek érdekében az alábbi jogosultságcsoportokat kell kialakítani a rögzítő rendszerben.

	Rendszer-gazda	Kiolvasó	Karbantartó	Biztonsági szakértő	Mozdony-vezető
Visszapillantó kamerák képei			Igen		Igen
Kamerák élő képének megjelenítése	-	-	Igen	Igen	
Felhasználók felvétele/törlése	Igen	-	-	-	
Jelszavak megadása/karbantartása	Igen	-	-	-	
Kiolvasás	-	Igen	-	Igen	
Időszinkron ellenőrzése	Igen	Igen	Igen	Igen	
Időszinkron beállítása	Igen	-	Igen	-	
Működés ellenőrzése	Igen	-	Igen	Igen	
Szelektív adattörlés	-	Igen	-	Igen	
Alkalmazói rendszer frissítése	Igen	-	Igen	-	
Eseménynapló ellenőrzése	Igen	-	-	Igen	

Az adatrögzítő szoftverét úgy kell kialakítani, hogy a kiolvasó számítógéphez (laptop) tartozzon egy szerepkör szerinti külső USB-s hardverkulcs egy 6 karakteres, ékezet nélküli nagy- és kisbetűket, illetve számjegyeket tartalmazó PIN kóddal, amellyel biztosítható megfelelő jogosultságú hozzáférés a rögzítő berendezéshez. A rendszerhez legalább húsz darab USB-s hardverkulcsot kell szállítani.

1.4. VK rendszer elemei

1.4.1. Központi egység

A VK rendszer esetében a központi egységnek csak a kamerák felügyeletét valamint azok képeinek a továbbítását a monitorokra kell megvalósítania. Csak azon monitorokon kell kameraképeket megjeleníteni, ahol a mozdonyvezető tartózkodik. A monitorokon az alábbiak alapján kell a képeket megjeleníteni:

- szerelvény haladása közben csak a menetiránnyal ellentétes irányba néző kamerák képeit kell a monitorokon megjeleníteni,
- ajtók nyitásakor valamennyi visszapillantós kamerát osztott képet alkalmazva kell megjeleníteni a monitorokon,

1.4.2. Kamera

Kültéri vandálbiztos, színes kamera, melyet a vasúti jármű külső falára kell rögzíteni. A kameráknak minden napszak idején is megfelelő minőségű képet kell szolgáltatnia. A vasúti üzemi körülményeknek (mechanikai, környezeti és villamos – melyek a megadott szabványokban rögzítettek) meg kell felelnie.

Felbontás:	legalább 960H vagy 720p
Kivitel:	vandálbiztos és legalább IP67-es ház, a vasúti jármű külső falára szerelhető kivitelnek megfelelő
Fényérzékenység:	Színes:0,1 lux/F2.0 vagy annál jobb
	Fekete-fehér: 0,01 lux/F2.0 vagy annál jobb
Elektronikus rekesz:	automatikus és 1/100,000-ig állítható
További specifikációk:	BLC, HLC, WDR (vagy HDR), AGC
Kamera lencse:	változtatható, legalább 3-12mm között

A szerelvény 66,87 m hosszúságú, amiből egy kamerával az első ajtótól a szerelvény közepéig terjedő területet kell megfigyelni, ami legalább 30 m hosszúságú. A megfigyelési terület felénél (kamerától mérten 15m távolságban) 250 pixel/méter legyen a kamera felbontása, valamint biztosítson arcfelismerést.

A megfigyelési terület sajátosságát figyelembe véve a kamerákat 9:16-os arányban kell telepíteni a szokványos 16:9-hez képest.

1.5. Vonatkozó vezérigazgatói utasítások

- Kivonat a 23/2014. (II. 12. MÁV-START Ért. 9.) VIG sz. vezérigazgatói utasítás a MÁV-START Zrt. Informatika Biztonsági Szabályzatáról
- Kivonat a 24/2014. (II. 12. MÁV-START Ért. 9.) VIG sz. vezérigazgatói utasítás a MÁV-START Zrt. Adatvédelmi Szabályzatáról
- Kivonat a 27/2014. (II. 12. MÁV-START Ért. 9.) VIG sz. vezérigazgatói utasítás a személyszállító vonatok biztonsági kamerarendszerével rögzített felvételek kezeléséről

Ezek a kivonatok a Műszaki Leírás 1. számú függelékét képezik.

1 számú függelék MÁV-START információvédelmi szabályzataiból kivonat

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

4.1.9. Adatbiztonság

Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek jelen utasítás, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik. A szerver számítógépek és a munkaállomások között személyes adatok kizárólag védetten (rejtjelezve) továbbíthatók.

A Társaságnál a dolgozók személyes adatait tartalmazó – az IHIR-t kiegészítő, vagy más, pl. a távbeszélőhasználat forgalmi adatait kezelő – adatbázist létrehozni a belső adatvédelmi felelős előzetes egyetértésével, a biztonsági vezető engedélyével szabad. Ugyanezen szabályok vonatkoznak az ügyféladatokat kezelő rendszerekre is.

Az ilyen adatbázist az üzleti titok védelmére előírt szabályokkal azonos kategóriájú (a Társaság Informatikai Biztonsági Szabályzatában – IBSZ – definiált ún. „fokozott") védelemben kell részesíteni. A rendszerekben a felhasználói jogosultságok korlátozásával biztosítani kell, hogy az egyes ügyintézők kizárólag a munkájukhoz feltétlenül szükséges személyes adatokat ismerhessék csak meg. A rendszereket a Társaság IBSZ-ében foglalt előírások szerint kell kifejleszteni, az ott előírt biztonsági okmányok elkészültét követően szabad használatba venni és üzemeltetni.

Személyes adat másolása az elektronikus adathordozók közül kizárólag CD-re és DVD-re megengedett, amin fel kell tüntetni a papír alapú adathordozóra előírt „Nem nyilvános" kezelési jelzést és az iktatószámot. Az így megjelölt dokumentumokat és adathordozókat biztonsági zárral ellátott fa iratszekrényben, vagy vas lemezszekrényben kell tárolni. A rontott és a munkapéldányokat megsemmisítésükig ugyanezen szabályok szerint kell tárolni; megsemmisítésük iratmegsemmisítővel / szétvagdosással történhet.

27/2014. (II. 12. MÁV-START Ért. 9.) sz. vezérigazgatói utasítás a személyszállító vonatok biztonsági kamerarendszerével rögzített felvételek kezelésének szabályzata

4.5. A képi adatok kiírása és a kiírás dokumentálása

A rögzítőberendezésből adatot kimásolni kizárólag a fentiek szerint kiállított Kiolvasási Megbízás alapján, a rajta feltüntetett adatokra kiterjedően engedélyezett.

A kiolvasáshoz a motorvonatokon egy mobil számítógépet kell a rögzítő-berendezéshez csatlakoztatni, a TALENT motorvonatokból kivett adattárolót pedig egy speciális dokkolóba kell helyezni. Ezt követően meg kell keresni a Kiolvasási Megbízáson közölt adatok alapján a kiírni szükséges felvételt (felvételeket), és a kérdéses adatokat ki kell másolni a mobil számítógépre, de a rögzítőberendezés merevlemezéről tilos letörölni. Ezt követően a kimásolt felvételeket (méretüktől függően) CD vagy DVD lemezre kell átírni.

A motorvonaton elhelyezett képrögzítő informatikai rendszer személyes adatokat tárol és kezel, ezért az illetéktelenektől fokozottan védeni kell a kiolvasáshoz használt mobil számítógépet, az adattárolókat, és az azokon lévő képi adatokat. A mobil számítógép fizikai védelméről és a rögzítőberendezés kulcsainak, valamint az IP címlistának a biztonságos, egymástól elkülönített tárolásáról a kiolvasást végző telephelyek vezetőinek kell gondoskodniuk. A kulcskezelés szabályait telephelyenként, a helyi sajátosságokat figyelembe véve kell meghatározni.

A technikai eszközök, valamint kulcsok kiadását és visszavételét dokumentáltan és visszakereshetően kell végezni. A rögzítőberendezés kulcsát és az IP címet kizárólag a kiolvasás és az adatállományok adathordozóra írásának idejére szabad átadni a kiírással megbízott munkatársnak.

<u>DVD-re, illetve CD-re elektronikusan fel kell írni:</u>

- a Kiolvasási Megbízáson megjelölt felvételt tartalmazó állomány(oka)t,
- a felvételek megnézésére szolgáló programot (külön mappában).

A DVD / CD ún. egyszer írható adathordozó legyen, amelyet írás után elektronikusan „le kell zárni” a további adatráírás megakadályozása érdekében.
Az adathordozón lévő adatok későbbi egyértelmű azonosítása érdekében annak dobozán (tasakján) tintával, emellett a lemez címkézett oldalán alkoholos filctollal fel kell tüntetni a következőket:

- a „Nem nyilvános” kezelési jelzés,
- a „…. sz. melléklet a …… iktatószámú anyaghoz” felirat (iktatószám: a hozzá tartozó Kiolvasási Megbízással megegyezően),
- a lemezre rögzített adatállomány(ok) neve.

Tilos az adathordozó külső felületén bármilyen személyes adatot feltüntetni. Az esetleg rontott adathordozót oly módon kell megsemmisíteni, hogy az adatok az eljárás után elérhetetlenek legyenek.

A kiolvasást végző a kimásolt adatokat nem ismerheti meg, csak az azokat tartalmazó elektronikus állományokkal dolgozhat. Sikeres DVD / CD-re írás után a mobil számítógépen tárolt képi adatokat oly módon kell törölni, hogy az adatok az eljárás után elérhetetlenek (felhasználói módszerekkel visszaállíthatatlanok) legyenek.

A kiírás megtörténtét a Kiolvasási Megbízás-on (annak alsó részén) kell rögzíteni, amit az adathordozóval együtt el kell juttatni a megbízóhoz.

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.

4.6.6. 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.

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.

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) dolgozók 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.

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.

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.

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 kötelessége. 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 **Ajánlati 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 követelményeit,
- 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.** (informatikai) 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 biztonsági 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.

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 állás szempontjából fokozott és 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 katasztrófa-esemény 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 kézikönyv(ekk)el. 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 munkahelyi 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.