Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara
1132 Budapest, Kádár u. 13.
Telefon: +36-1-422-0079 - Fax: +36-1-220-8921

Tisztelt Kolléga!

Az alább olvasható kamarai szakmai ajánlást abból a célból készítettük el, hogy a vagyonvédelmi ágazatban dolgozók iránymutatást kapjanak a munkájuk végzéséhez. Nem jogászkodunk, a tagságot akarjuk segíteni. Az ajánlás természetesen még nem teljes körű. Tervezzük egy példatár összeállítását is mindenki tájékoztatására. Az élet produkálhat eddig ismeretlen dolgokat, de az Ön segítsége is kell ahhoz, hogy a szakmában dolgozók okulhassanak, magasabb szintű munkát végezhessenek.

Kérem, írja meg véleményét, mivel egészítsük ki, milyen módosítási javaslatai vannak: *kollegium@szakmaikamara.hu*

Távfelügyeleti rendszer minőségi kritériumai

Grade 2 Biztonsági fokozat

Készült Magyarország Vagyon-Életvédelmi és Tűz távfelügyeleti szolgálatást nyújtó rendőrhatósági engedéllyel rendelkező vállalkozásainak

Ezen dokumentum alapjául szolgál az EN-50136 szabvány, kifejezetten az EN-50136-1-1 („Riasztás átviteli és fogadó rendszerek általános követelményei”) és az EN-50136-7 („Riasztás átviteli és fogadó rendszerek alkalmazási irányelvei”)

Bevezető

- Ez a legelterjedtebb, legáltalánosabban felhasznált kisüzleti, lakossági távfelügyeleti és helyi biztonsági rendszerre vonatkozó védelmi fokozat.
- Az EN- szabványos követelmények adottak, melyek a 2. biztonsági fokozatnak felelhetnek meg.
- A szabvány szerint a kialakítást együtt kell vizsgálni a helyi figyelemfelhívó eszközökkel és a behatolásjelző rendszer kialakításával-telepítésével. (Hang-Fény jelzők, átjelzés, kialakítás, héj-és térvédelem)
- A megadott elvárások a szabvány előírásai alapján készültek, annak tételes felsorolása nélkül.

Közcélú vezetékes távbeszélő/adatkommunikációs hálózathoz csatlakoztatott digitális kommunikátorral biztosított távfelügyelet

Elektronikus védelem használata esetén a behatolás-jelző rendszer által adott riasztás-jelzés célja a védett objektum mielőbbi biztosítása, melyet leginkább az élőerős beavatkozás kezdeményezése tesz megfelelővé. Mivel az elriasztás sikere esetleges, alapvetően az élőerős beavatkozásra kell támaszkodni.

Egy megfelelően kialakított riasztás-átviteli rendszer elegendő információt szolgáltat a felügyelt objektum behatolás-jelző rendszerének rendelkezésre állásáról, a jelzésekről, valamint képes támogatni a gyors és sikeres élőerős beavatkozást.

A riasztás-átviteli rendszer elemei:

- a felügyelt objektum adó/vevője,
- átviteli rendszer,
- távfelügyeleti központ:
  - riasztás-fogadó központ,
  - riasztás-megjelenítő berendezés,
  - diszpécser szolgálat,

1. A felügyelt objektumban telepített digitális kommunikátor

A behatolás-jelző rendszereket a kockázat szintje alapján a szabvány fokozatokba sorolja (Grade1, Grade2, Grade3 és Grade4), melyet az alkalmazott riasztás-átviteli rendszernek is figyelembe kell vennie. A fokozatokat a szabvány alapvetően a várható támadó felkészültsége szerint határozza meg, de ez elég szoros összefüggésben van a biztosítók megközelítésével, amely az objektumban található értékek nagyságát tekinti kiinduló alapnak.

Az egy átjelzési útvonalon teljesülő távfelügyeleti rendszer legfeljebb a szabvány 2. biztonsági fokozata, vagyis az alacsony, ill. közepes közötti kockázat szintjét képes teljesíteni, tehát tipikusan lakossági felhasználásra ajánlott. Ebben a kategóriában feltétlen elvárás kültéri, 100 dB(A) akusztikus jelszintű, szabotázsvédett, saját akkumulátorral rendelkező hangjelző-fényjelző eszköz egyidejű alkalmazása is!

A kommunikátor több esetben része a behatolás-jelző központnak, máskor utólag illesztik hozzá. A közcélú távbeszélő hálózathoz csatlakoztatott kommunikátornak az ETS 300 001 szabványnak és az EN-50131 szabvány Grade2 biztonsági fokozatának kell megfelelnie.

A telepítés során biztosítani kell, hogy a kommunikátort, amennyiben közcélú vezetékes analóg vagy digitális telefonvonalon történik az átjelzés, az objektumban található egyéb távközlési eszközök elé (telefon, fax, üzenetrögzítő) fix bekötéssel csatlakoztassák és a behatolás-jelző központ felügyelje a vonali feszültség meglétét. A feszültség hiánya esetén élesített állapotban a rendszer a helyi hang és fényjelző eszköz(ök) aktívvá válásával jelezze a külvilágnak a riasztást, esetleges szabotázs fennállását.

Ha a kommunikátor tápellátását a behatolás-jelző központ biztosítja a másodlagos tápáramforrásnak (akkumulátor) 12 óra, külső táplálás esetén 24 óra üzemet kell biztosítania az elsődleges táplálást biztosító elektromos hálózat kiesése után.

2. Átviteli út

Átviteli út alatt a felügyelt objektumban telepített kommunikátor és a távfelügyeleti központban telepített riasztás-fogadó központ közötti távközlési összeköttetés értendő. Esetünkben közcélú vezetékes kapcsolt távbeszélő hálózat biztosítja a kapcsolatot, amely paramétereinek befolyásolására kevés lehetőség van, de rendelkezésre állása tipikusan 98%, amely megfelel a 2. biztonsági fokozatú rendszerekkel szemben támasztott követelményeknek. A GPRS rendszerek rendelkezésre állása a legtöbb esetben 96%, ami az 1. biztonsági fokozatnak felel meg. Amennyiben az átjelzés (átjelzési formától és eszköztől függetlenül) tudja biztosítani a 98%-ot, abban az esetben megfelel a 2. Biztonsági szintnek.

A felügyelt objektum kommunikátorát úgy kell csatlakoztatni, hogy a távbeszélő hálózat kapcsolóközpontja felé menő szakaszon semmilyen berendezés ne tudja a kommunikátor tárcsázását, ill. a riasztás átvitelét megszakítani.

A távfelügyeleti központban telepített riasztásfogadó adó/vevőhöz csatlakozó vonalat kizárólag riasztás-fogadásra szabad használni és a vonali feszültséget felügyelni kell. A távközlési szolgáltatóval kötött szerződésben a hívószámot titkosítani kell és biztosítani kell a ráhívással való foglalttá tétel elleni védelmet.

Az átviteli út állapotát a felügyelt objektumban telepített kommunikátor által legalább 24 óránként küldött életjellel kell ellenőrizni.

3. Távfelügyeleti központ

3.1. Riasztásfogadó adó/vevő

A riasztásfogadó adó/vevő legalább az alábbi, a felügyelt objektumtól érkező jelentéseket fogadja:

- felügyelt objektum azonosítása;
- behatolás-jelző rendszer állapota (Nyitás-Zárás)
- riasztás (típusa, terület, zóna, ill. érzékelő megadása);
- hibaállapot;
- tápfeszültség-kimaradás, valamint a másodlagos táplálás kiesése.

A riasztásfogadó adó/vevő rögzítse és tárolja a fogadott jelentéseket és azok vételét igazoló nyugtázás tényét. A riasztásfogadó adó/vevő elsődleges táplálását az elektromos hálózatról kapja és rendelkeznie kell annak kiesése esetén az üzemeltetést szünetmentesen további 30 percen keresztül biztosító másodlagos táplálással.

Alapfogalmak:

Távfelügyelet: Egy olyan két végpont között kialakított, rendszerint folyamatos kapcsolat, mely esetén az adó oldali elektronikai rendszer által küldött jelzések a vevő oldalon – folyamatosan- szünetmentesen fogadják a jelzéseket, majd a megfelelő intézkedések megtörténnek a jelzés értelmezését követően.

Helyiségek:

Távfelügyeleti központ: (ARC) Egy zárt helyiség-terület, ahol a beérkezett jelzések értelmezése és az azokra történő reagálás zajlik.

Szerverszoba (terem): Egy olyan fizikailag lezárt egység, terület – ahová csak a rendszergazda (és helyettese) és a biztonsági koordinátor (és helyettese) léphet be. Távfelügyeleti diszpécser normál esetben nem.

Eszközök:

Távfelügyeleti vevő: Egy olyan, speciálisan behatolás (esetenként tűz) jelzőrendszerek fogadására gyártott, minősített informatikai eszköz, mely többféle kommunikációs protokollon és útvonalon fogadja a beérkező jelzéseket.

Távfelügyeleti adó/vevő (ATS) (átjelző eszköz): Az ügyfélnél kihelyezett, (a saját specifikációjú kommunikációs útvonallal rendelkező) hardver, mely a behatolás (vagy tűz) jelzőrendszer kommunikációs ki/bemeneteire csatlakozik és kommunikáció esetén üzemszerűen továbbítja azt a távfelügyelei központnál (lévő szerverszobában - teremben) elhelyezett távfelügyeleti vevőnek a szükséges kommunikációs protokollban az információt.

Kommunikációs protokoll: A behatolás (esetenként Tűz) jelzőrendszerek kommunikációjára kifejlesztett, szabványosított egységes kódtábla rendszer, melyektől bizonyos esetekben egyénenként el lehet térni. A leggyakoribb formái: Ademco által használt CID (Contact IDentification), SIA (Security Indsutry Authority), 4/2,

Kommunikációs útvonal: Az ügyfélnél elhelyezett adóegység és a távfelügyeleti vevő közti kommunikációs csatorna. Ez, a szolgáltatási típus megrendelésétől és a kiépített technikai viszonyoktól függően az alábbi útvonalakat foglalja magában: Analóg kapcsolt telefonvonali átjelzés, Rádiósfrekvenciás átjelzés (egyedi bérelt hullámhosszon), GSM sávon történő átjelzés, GPRS hálózaton történő jeltovábbítás, Vezetékes internet (IP) alapon történő jeltovábbítás

Szoftver: Egy olyan kézzel meg nem fogható szellemi termék, mely -a felhasználó igényeit szem előtt tartva- segít az adott eszközt (hardvert) üzemszerűen használni.
„A szoftver (angol: software) alatt a legszűkebb értelemben elektronikus adatfeldolgozó berendezések (például számítógépek) memóriájában elhelyezkedő, azokat működtető programokat értünk.” Forrás: Wikipédia

Mindennapi szoftver példa: MS Office

Távfelügyeleti szoftver: Egy olyan szoftver, mely képes a szabványos és egyedi kommunikációs protokollok alapján a kommunikációs csatornákon beérkezett és a távfelügyeleti vevő által nyugtázott jelzéseket a távfelügyeleti diszpécser(ek) számára érthető magyar nyelvű információvá tenni. Példa: SIMS, OGS

Személyi fogalmak:

Távfelügyeleti diszpécser (operátor): Az a büntetlen előélettel rendelkező személy(zet), mely a beérkezett és már tárolt jelzések alapján intézkedéseket tesz a vagyon-élet és testi épség megóvása céljából.

Távfelügyeleti adminisztrátor: Az a büntetlen előélettel rendelkező személy, aki rendelkezik olyan jogkörrel, mely a távfelügyeleti szolgáltatást igénybe vevő ügyfelek adatait módosíthatja, felülírja, rögzíti, de nem törölhet!
(A távfelügyeleti diszpécser ezen jogkörrel nem felruházható.)

Rendszergazda: Az a büntetlen előéletű informatikában jártas személy, aki a távfelügyeleti központ vevő egységeit, szervereit, munkaállomásait valamint minden egyéb ezekhez szorosan kapcsolódó informatikai berendezést (Pl. Routerek, Swichek,stb.) karbantart, javít, ellenőriz.

Biztonsági koordinátor: Az a büntetlen előéltű személy, aki rendelkezik biztonságtechnikai szerelésre jogosító hasági igazolvánnyal. Ezen személy felel a távfelügyeleti központban elhelyezett elektronikus védelmi megoldások kifogástalan működéséért.

- Végzettséget és munkakört illetően a rendszergazda és a biztonsági koordinátor szükség szerint azonos ember is lehet.

Az elvárási kritériumok (az EN-50136 alkalmazásával) a következő öt pont alapján vannak osztályozva a 2. Biztonsági szintnek megfelelően:

- Az ARC –ben működő informatikai rendszer, informatikai biztonság
- A redundancia (szoftver és hardver)
- A távfelügyeleti szoftver, a megjelenítés paraméterei és tulajdonságai
- Az adatkezelés és adattárolás
- Az ARC –ben elhelyezett távfelügyeleti vevők és az intézkedésköteles jelzésekre reagáló személyzet (diszpécser-ek) személyi-védelme

1. Az ARC –ben működő informatikai rendszer, informatikai biztonság

- *1.1 A távfelügyeleti vevő egység(ek), szerver(ek) a távfelügyeleti diszpécsertől elzárt, külön erre a célra kialakított egyszerű mechanikai (zárható) és 0-24 minimum EN-50131 Grade 2 elektronikai védelem alatt álló Rack-szekrényben vagy külön helyiségben kerülhetnek elhelyezésre. A távfelügyeleti diszpécser nem tudhatja ezen elektronikai védelmet hatástalanítani, de amennyiben Vis Maior esetén hozzá kell férjen a szerverhez, vevő(k)höz, bejutást kell neki biztosítani. Ezen riasztási esemény(ek)ről az elektronikai jelzőrendszernek hangos riasztást kell adnia és ezen kritériumoknak megfelelt partner ügyeletnél intézkedésköteles jelzést kell generálnia.*

- *1.2 A távfelügyeleti vevőegység(ek) hez csatlakozó szerver(ek) szintén ebben a védett rack-szekrényben helyezkedhetnek el. (Ügyelve a szellőzésre.)*

- *1.3 A távfelügyeleti szerverhez távolról (frissítés, újraindítás) a rendszergazda egy külön, erre a célra kialakított titkosított csatornán (pl: SSH, VPN) keresztül férhet csak hozzá. Minden ilyen távolról történő hozzáférésről napló kell készüljön. Az Információbiztonsági szint I1.*

- *1.4 Munkaállomásnak használt PC-n az egéren és billentyűzeten kívüli USB portokat le ke kell tiltani.*

- *1.5 Az EN-50136-7 4.5.6.) bekezdése szerinti ún. „Éberségfigyelést” kell alkalmazni azon esetben, ha előfordul olyan helyzet, amikor csak egy személy tartózkodik huzamosabb ideig az ARC riasztásmegjelenítő és feldolgozó munkaállomásainál. Amennyiben az „éberségfigyelés funkció” aktiválódik, az ügyeletvezetőnek, a biztonsági koordinátornak, írásos figyelmeztetést kell adjon a rendszer. (pl.: E-Mail küldése, pontos idővel és eseményekkel)*

- *1.6 Az Informatikai rendszer – belső hálózat I1-es védelmét kell biztosítani (EN-50136-7) szerint, azaz külsőleg nem hozzáférhető és nem olvashatóak az adatok, melyek ezen a csatornán futnak.*

- *1.7 Amennyiben a távfelügyeleti vevő(k) leesnek a hálózatról, figyelmeztető jelzéseknek kell aktiválódniuk az EN-50136-4 4.16 bekezdése szerint.*

2. A redundancia (szoftver és hardver)

- *2.1 Az a szerver és minden egyéb olyan informatikai és hálózati eszköz melyek közrejátszanak egy adatátviteli vagy feldolgozási folyamatban, a hálózati feszültség kimaradását követően minimum 60 percig szünetmentesen kell ellátniuk a feladatukat.*

- *2.2 A 2.1-ben foglaltaknak megfelelően informatikai eszköznek minősül a távfelügyeleti vevő, melynek a fentiektől eltérően minimum 30 percig kell ellátnia a feladatát.*

- *2.3 A távfelügyeleti vevő(k)nek rendelkeznie kell magyar nyelvű LCD kijelzővel.*

- *2.4 Minden olyan kommunikációs átjelzési útvonal, mely a távfelügyeleti vevőegységbe közvetlen-vagy közvetetten érkezik meg, pl.: vezetékes internet, csak FIX IP címmel ellátott lehet, valamint ezen internetek beérkezési útvonalát bizosító hardverek tápellátását (swich-ek, routerek) minimum 60 percig szünetmentessé kell tenni.*

  Megj.: Amennyiben a távfelügyelet ún. kihelyezett „sziget” rendszer alapján működik, úgy a „szigeteket” szolgáltató főbb szerverek, informatikai eszközök, átjelzést fogadó, továbbadó informatikai eszközök, az ezeket elhelyező terület - elektronikus és mechanikus védelme és a „kihelyezett szigetek” (ARC) védelme, ezen elvek kritériumjainak kell megfeleljenek.

- *2.5 - A 2.4-ben foglaltaknak megfelelően a távfelügyeleti vevőkészüléknek (és a szoftvernek) értelmezhető hibajelzést kell leadnia a diszpécserközpont azaz a távfelügyeleti szoftver felé valamely első/vagy másodútvonali kommunikációs csatorna megszakadásáról. Ezen hibajelzések alapján (belső v- saját generálású hibák) a diszpécsereknek rendelkeznie kell, egy minden vállalkozás által önállóan kidolgozott „Vis Maior” intézkedési renddel. A kiadott hibaüzenet(ek) jól értelmezhető legyen és kellő hanghatással kell rendelkeznie.*

- 2.6 *Amennyiben a távfelügyeleti szoftver valamiért meghibásodik, használhatatlanná válik, akkor WEB felületen biztosítani kell a GPRS kommunikációval rendelkező eszközök vevőegység(ei) által regisztált jelzések adatainak kiolvasását és aszerint megtenni a szükséges intézkedéseket.*

(Vis Maior helyzetben a diszpécserszolgálat egy lezárt (pecsételt és aláírt) borítékban lévő bejutási eszközzel léphet be a szerverszobába, melyről riasztási esemény történik.) Erről az eseményről a partner ügyeletnek értesülnie kell. (Távfelügyelt szerverszoba – Rack szekrény behatolásjelzőjének eseményeiből)

- 2.7 *Amennyiben a szerver – vagy – szerverek szoftverfrissítést, hardveri javítást valamint egyéb olyan műszaki állapotot előidéző helyzetet hoznak létre, mely az adott szerveren történő információáramlást megakadályozza úgy azokat az információkat a WEB-es felületén keresztül (ha van ilyen) folyamatosan figyelni kell, majd a beérkező jelzésekre intézkedni. Ezen irányelv pontja olyan üzemszünet, előre betervezett kimaradásra vonatkozik, mely nem számítható Vis Maiornak.*

- *2.8 A védett objektumnál elhelyezett ATS, a helyszínnek megfelelő biztonsági fokozattal rendelkezzen (EN-50131) és az ATS re vonatkozóan az EN-50136-2-1-nek megfelelően. Grade2*

- *2.9 Az ATS Követelményei (Átjelzési idő, sebesség) és az esetleges bérelt útvonali átjelzés, valamint az analóg, kapcsolt vonali átjelzés és hálózat feleljen meg az EN-50136-2-3 szabványnak. – Kapcsolt vonali átjelzés esetén. Ezen pont a helyszínen található eszközökre és azok kialakítására vonatkozik.*

3. A Távfelügyeleti szoftver, a megjelenítés paraméterei és tulajdonságai

- *3.1 A Távfelügyeleti szoftverbe be vagy ki lépni jelszó és azonosító nélkül nem lehet. Nem elfogadott az egyszerűen kitalálható jelszó.*
  Pl.:1222 vagy 1234 vagy 1111, stb.

- *3.2 A Távfelügyeleti belépő jelszó minimum 8 karaktert tartalmazzon, melyben betű és szám egyaránt szerepeljen.*

- *3.3 A Távfelügyeleti szoftverből a diszpécser nem olvashat ki olyan információkat naplózatlanul – teljesen nyomtalanul, mint pl.: a behat. rendszer mérnöki kódja. Ezeknek olyan helyen is visszatekintendően kell megjelenniük, mint az ügyfél elmúlt eseményei.*

- *3.4 A Távfelügyeleti szoftverben minden egyes elindított parancsot (keresés, megtekintés, adatmódosítás, stb...) egy olyan felületen kell „log"-olni és folyamatosan tárolni, melyhez csak a rendszergazda férhet hozzá. A „log" -olásnak tartalmaznia kell a pontos időt-dátumot, diszpécser nevet vagy azonosítót a munkaállomás számát és a „log"olt esemény egyértelmű magyar megnevezését.*

- *3.5 A Távfelügyeleti szoftver hangjelzés nélkül nem közölhet azonnal intézendő információt a diszpécserrel.*

- *3.6 A Távfelügyeleti szoftverben nem megengedhető ideiglenesen sem olyan diszpécsernek jogot adni adatmódosításra, aki nem „admin vagy supervisor" szintű jogosult.*

- *3.7 A Távfelügyeleti diszpécser (operátor) szoftverileg nem iktathat ki folyamatos kiiktatásra egy ügyfelet sem, maximum ideiglenes állapotra, mely nem haladhatja meg a 24 órát.*

- *3.8 A Távfelügyeleti szoftver csak akkor –engedélyezhet- adhat „nyugta” jelzést a vevőnek, ha a beérkezett jelzés adata(i) mentésre került(ek) egy adatbázisban.*

4. Az adatkezelés és adattárolás

- *4.1 A jelenleg hatályban lévő minden jogszabály betartásával kezeljük és tároljuk a meglévő és új adatokat. (Ha szükséges, akkor TÜK helyiség.)*

- *4.2 Bármilyen adat kiadása, melyre minden vállalkozás saját maga szabja meg a kiadható adatok listáját – telefonon keresztül – azonosító jelszó nélkül és a jelszó szintjének meghatározása nélkül nem történhet. Ügyeljünk az adatvédelmi törvényre és a jogszabályok betartására!*

- *4.3 A távfelügyeletnek kifelé telefonáláskor nem elég arról a hívószámról telefonálnia, amelyről a hívás valószínűleg kezdeményezve lesz sok alkalommal és ezt a szerződésben is rögzítették, hanem amennyiben az ügyfél úgy döntött, legyen lehetőség egy olyan jelszó használatára, mellyel az esetleges azonosító jelszó kicsalását meg lehet akadályozni és az ügyféllel történt beszélgetés kezdetén (távfelügyeletről kitelefonálás esetén) először a diszpécser azonosítja magát az ügyfélnek.*

  (Mindig az mondd előbb jelszót aki a telefonhívást kezdeményezte.)

- *4.4 Bármilyen telefonon történő intézkedésre történő felkérés – megszakítás, stb... csak olyan hangcsatornán történhet, mely a jogszabályokban előírtaknak megfelelően hangrögzítésre kerül.*

- *4.5 A Vállalkozásnak regisztráltnak kell lennie a NAIH –ban és minden (akár egyénileg az ÁSzF-ben és ezen felül), a jogszabályokban foglaltaknak megfelelően meg kell feleljen adatkezelés, tárolás szempontjából.*

5. Az ARC –ben elhelyezett távfelügyeleti vevők és az intézkedésköteles jelzésekre reagáló személyzet (operátorok) személyi-védelme

- *5.1 A távfelügyeleti diszpécserközpontnak külső tértől fizikailag (mechanikai és elektronikai védelmet használva) elzártnak kell lennie, kívülről belátni azon monitorokra (melyeken bármilyen személyes adat és/vagy a távfelügyeleti szoftver fut) ne lehessen.*

- *5.2 Minden diszpécseri munkaállomásnál legalább egy személyi támadásjelző egységnek kell lennie.*

  - *5.2.1. A támadásjelző egység(ek)nek folyamatos 0-24 távfelügyeleti védelem alatt kell állniuk, olyan távfelügyelethez csatlakoztatva, amely ezen irányelveknek megfelel.*

  - *5.2.2. Rádiós támadásjelző egység esetén a rádiós adó-vevő egységnek ugrókódos kialakításúnak kell lennie.*

- *5.2.3 A Rádiós támadásjelző egység(ek)nek és az átjelzést biztosító egységeknek legalább 360 percig szünetmentesnek kell lennie. (Pl.:Szabotázsvédett segéd tápegység)*

- *5.2.4 A támadásjelző egységeket havonta tesztelni kell a biztonsági koordinátornak. (Távfelügyeleti átjelzés – eszközstabilitás)*

- *5.3 A diszpécserközpontba történő belépés beléptetőrendszerrel ellenőrzötten kell, hogy történjen. Önálló olvasó/vezérlő és egyszerű kódzár nem megengedett. A beléptető rendszer olvasóinak biztonsági szintjének megfelelősége minimum a több bites titkosítás a kártya és olvasó között 125KHz en működő olvasóknál is. A beléptetőrendszerekre vonatkozó telepítési elvárásoknak megfelelően járjunk el. Pl: síkmágnes esetén ügyeljünk a menekülés biztosítására. (zöld színű vésznyitó) A rendszer kiépítésénél vegyük figyelembe az EN-50133 szabványsorozatot. („Beléptető rendszerek")*

- *5.4 A szerverszoba – rack szekrény – elektronikai védelmének meg kell felelnie az EN-50131(„behatolásjelző rendszerek") szabványai által előírt Grade 2 védelmi fokozatnak.*

- *5.5 Amennyiben egy műszakban egy időben csak egy ügyeletes dolgozik, úgy a személyi támadásjelzésre szolgáló egységen kívül még rendelkeznie kell az ügyeletnek egy egészségügyi segélyhívó egységgel is, melyre a partnerügyeleten minden információ megtalálható arról, hogy ilyenkor kit és hogyan kell értesíteni.*

- *5.6 Az 5.5-ben meghatározott támadás és segélykérés jelző egységeknek szín alapján is el kell térniük. A megkülönböztetés egyértelmű legyen. Pl.: Rádiós adóknál – Piros gombos a támadásjelző és sárga vagy zöld gombos a segélykérő.*

- *5.7 Az a távfelügyelet (partnerügyelet) mely 0-24 órában távfelügyeli a támadásjelzéseket, segélyjelzéseket, szervervédelmet szolgáló behat.jelzőt, ezen irányelvek minden pontjának meg kell feleljen.*

- *5.8 Az „ARC" –ba belépő-kilépő személyek azonosságát, valamint az „ARC" -ben történtekről folyamatosan rögzített videó felvétel szükséges. Ezen videó rendszernek hálózati áramkimaradás esetén minimum 60 percig szünetmentesnek kell lennie. Ezen felvett adatokhoz és tárolásához a mindenkor érvényben lévő jogszabályok betartása kötelező, valamint csak az arra kijelölt adatkezelő férhet hozzá. (Adatvédelmi törvény!)*
  A video rendszer kialakításánál vegyük figyelembe az EN-50132 szabványsorozatot. (CCTV – Video Megfigyelő rendszerek)

Összeállította:
- *Kerekes János - kjszakerto@gmail.com*
- *Móré Attila - amore@tvt.hu*
- *Tóth Attila - atoth@tvt.hu*
- *Doktorits László - doktorits.laszlo@objekt-or.hu*