

**JÁSZBERÉNYI VAGYONKEZELŐ ÉS VÁROSÜZEMELTETŐ
NONPROFIT ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG**



**Térfigyelő kamera rendszer adatkezelési szabályzata és eljárásrendje
változásokkal egységes szerkezetben**

Jászberény, 2026.02.16

Hatályos: 2026.02.16 - től

(A korábban e témakörben kiadott Szabályzat a fenti naptól hatályát veszti.)

Készítette:

Dr. Sümei Zsombor sk. DPO

Véleményezte: Kalics József kontrollingvezető, megfelelési tanácsadó

Jóváhagyta:

Horgosi Zsolt vezérigazgató

1.	A szabályzat tartalma	4
2.	A szabályzat célja, hatálya, figyelembe veendő előírások	4
2.1.	A szabályzat célja	4
2.2.	A szabályzat hatálya	4
2.3.	Jogszabályi háttér	4
3.	Értelmező rendelkezések	5
4.	A területi térfigyelő kamera rendszer	6
4.1.	A rendszer felépítése	6
4.1.1.	A területre kihelyezett kamerák.....	7
4.1.2.	Tájékoztatás.....	7
4.1.3.	A központi helyiség.....	8
4.1.4.	A felvételek megtekintése	8
4.2.	A rendszer üzemeltetési rendje.....	8
4.2.1.	A rendszer üzemeltetésének célja.....	8
4.2.2.	A rendszer tulajdonosa és üzemeltetője.....	8
4.2.3.	A Térfigyelő területi térfigyelő kamera rendszer üzemeltetése.....	9
4.2.4.	A rögzített felvételek visszánézése.....	9
	Felvételek törlése: Ld. 5.5 Az adatkezelés időtartalma, az adatok törlése	9
4.2.5.	Eljárás indítása, illetve kezdeményezése.....	9
5.	A területi térfigyelő kamera rendszerrel kapcsolatos adatkezelés	9
5.1.	A területi térfigyelő kamera rendszer által rögzített felvételek, mint személyes adatok	10
5.2.	Az adatkezelés alapelvei.....	10
5.3.	Az adatkezelés jogalapja.....	10
5.4.	Az adatkezelés korlátai	10
5.5.	Az adatkezelés időtartalma, az adatok törlése	11
5.6.	Betekintési jog	12
6.	Adatbiztonság.....	12
6.1.	Szervezési intézkedések.....	12
6.1.1.	Jogosultságok	12
6.1.2.	Üzembiztonság	14
6.1.3.	Adattovábbítás.....	15
6.2.	Technikai intézkedések és beállítások	15
6.3.	Információcsere	17
6.4.	Kockázatmonitorozás és folyamatos felügyelet	17
6.5.	Változáskezelés és előzetes információbiztonsági hatásvizsgálat	18
6.6.	Egységes biztonsági konfigurációk	19

7.	Nyilvántartás vezetési kötelezettség.....	21
7.1.	Kamera nyilvántartás.....	21
7.2.	Üzemeltetési napló	22
7.3.	Megfigyelési napló	22
7.4.	Visszanézési napló.....	22
7.5.	Az adathordozók nyilvántartása	22
7.6.	Adat másolási napló.....	23
7.7.	Adattovábbítási napló	23
7.8.	Felvételek megsemmisítésének nyilvántartása	23
7.9.	Incidens nyilvántartás	23
8.	Feladat- és hatáskörök	24
8.1.	Az ellenőrző személyzet vezetőjének adatkezelési feladat- és hatásköre.....	24
8.2.	A terület-felügyelő adatkezelési feladat- és hatásköre	24
8.3.	Beállítások kezelése, admin felhasználó feladatai	24
9.	A szabályzat tartalmának megismertetése	25
10.	Záró rendelkezések	25
1.	melléklet - Éves Biztonsági Értékelési Terv és Eljárásrend	27
2.	melléklet - Kamerák negyedéves ellenőrzés jkv	33
3.	melléklet Területi térfigyelő kamera rendszer felvételeinek lekérése és hozzáférése	35

A Jászberényi V.V. Nonprofit Zrt. (a továbbiakban Szervezet) az általa jogos érdekből működtetett területi térfigyelő kamera rendszer adatkezelési szabályait az alábbiak szerint határozza meg. A kamerák által megfigyelt helyszínek címei a jelen dokumentum mellékletét képező, a kamerák pontos elhelyezkedését megjelenítő táblázatokban kerültek feltüntetésre.

1. A szabályzat tartalma

A szabályzat tartalmazza:

- a szabályzat céljának, hatályának meghatározását, a figyelembe veendő előírásokat.

Jelen dokumentum a 7/2024. (VI.24.) MK rendelet szerinti rendszerbiztonsági tervként is szolgál.

2. A szabályzat célja, hatálya, figyelembe veendő előírások

2.1. A szabályzat célja

A szabályzat célja, hogy részletesen meghatározza a térfigyelő kamera rendszer működtetésével kapcsolatos adatkezelési szabályokat, különösen:

- az adatrögzítésre vonatkozó szabályokat,
- a rögzített adatok felhasználásának előírásait,
- az adattovábbítási, és betekintési jogok rendjét,
- az adattörlési kötelezettséget.

2.2. A szabályzat hatálya

A szabályzat személyi hatálya kiterjed elsősorban a Szervezet első számú vezetőjére, az őt helyettesítő személyre, illetve az e témában megbízottként eljáró vezetőkre, szakmai vezetőkre.

2.3. Jogszabályi háttér

A szabályzat elkészítésekor figyelembe vett tagállami vagy uniós jogszabályok:

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, (továbbiakban: Infotv.)
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (továbbiakban: Szvtv.)
- 2012. évi I. törvény a munka törvénykönyvéről (továbbiakban Mt.)
- az Európai Parlament és a Tanács 2016/679 számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló rendelete (általános adatvédelmi rendelet, továbbiakban: GDPR)
- A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről
- A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről

3. Értelmező rendelkezések

A szabályzat alkalmazásában az egyes fogalmakon a következőket kell érteni:

Térfigyelő kamera rendszer

A térfigyelő kamera rendszer: azok az eszközök és megoldások, melyek kamerák kihelyezésével és üzemeltetésével lehetővé teszik a terület távolból történő megfigyelését, a kamerákkal képfelvételek készítését, a felvételek tárolását, valamint az adatok továbbítását.

Ellenőrző személyzet

Egyrésztől lehet adatkezelő belső szervezeti egységként létrehozott egység, jelen esetben az adatkezelő vezetője és megbízottja. Az erre a feladatra kijelölt munkavállaló állandó vagy ideiglenes jelleggel személyt, meghatározott területet, létesítményt vagy értéket őriz, véd, illetve ellenőriz, az elektronikus megfigyelőrendszer működése útján kép-, hang-, valamint kép- és hangfelvételt az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti adatvédelmi jogok érvényesítése mellett, illetve e törvényben meghatározott korlátozó rendelkezések betartásával készíthet, illetve kezelhet. Másrésztől az ellenőrző személyzet (ellenőrző személyzet) lehet az a szolgálati forma, amely során az erre a feladatra kijelölt alvállalkozó munkavállalója (továbbiakban vagyonőr) az őrhelyén (felállítási helyen és mozgási körzetben) állandó vagy ideiglenes jelleggel személyt, meghatározott területet, létesítményt vagy értéket őriz, véd, illetve közbiztonsági szempontból ellenőriz. A vagyonőr az elektronikus megfigyelőrendszer működése útján kép-, hang-, valamint kép- és hangfelvételt a kötelezettségeit meghatározó szerződés keretei között, a szerződésből fakadó kötelezettségei teljesítése céljából, az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti adatvédelmi jogok érvényesítése mellett, illetve e törvényben meghatározott korlátozó rendelkezések betartásával készíthet, illetve kezelhet. E tevékenysége során vagyonőrzési feladatokat ellátó személy adatkezelőnek minősül.

Terület

A Szervezet illetékességi területén lévő olyan terület, mely az ingatlan nyilvántartásban a Szervezet által használt földrészletként (vagy azon belüli üzemi területként) beazonosítható.

Személyes adat

Személyes adat - az Infotv. 3. § 2. pontja szerinti 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.

Adatkezelő

Adatkezelő - az Infotv. 3. § 9. pontja szerinti adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

Adatkezelés

Adatkezelés - az Infotv. 3. § 10. pontja szerinti adatkezelés: az alkalmazott eljárástól függetlenül az adaton 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 adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Adattovábbítás

Adattovábbítás - az Infotv. 3. § 11. pontja szerinti adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Adattörlés

Adattörlés - az Infotv. 3. § 13. pontja szerinti adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

Adatmegsemmisítés

Adatmegsemmisítés - az Infotv. 3. § 16. pontja szerinti adattörlés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.

Adatfeldolgozó

Adatfeldolgozó - az Infotv. 3. § 18. pontja szerinti adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi.

4. A területi térfigyelő kamera rendszer

4.1. A rendszer felépítése

A szervezet meghatározza a területi térfigyelő kamera rendszer azon rendszerelemeit és rendszerelem-kategóriáit, amelyek belső rendszerkapcsolatot igényelnek az elektronikus információs rendszer megfelelő működéséhez. A belső kapcsolatot igénylő rendszerelemek köre az alábbi:

- Kamerák – a kép- és metaadatok rögzítő felé történő továbbításához;

- Rögzítőegység (NVR/DVR) – a kamerák által küldött adat fogadásához, feldolgozásához és tárolásához;
- Helyi megjelenítő vagy kezelőfelület (ha van) – a rögzítő közvetlen eléréséhez és a felvételek visszanézéséhez.

A meghatározott rendszerelemek közötti kapcsolat zárt, belső, közvetlen fizikai adatkapcsolat, amely nem kapcsolódik külső hálózathoz, és kizárólag a területi térfigyelő kamera rendszer működéséhez szükséges adatátvitelre korlátozódik. A szervezet biztosítja, hogy ezen kapcsolatok engedélyezése, dokumentálása, felülvizsgálata és szükség esetén megszüntetése a vonatkozó biztonsági követelményeknek megfelelően történjen. A rendszer biztonsági osztályba sorolása, bizalmasság-sértetlenség-rendelkezésre állás értékelése az EIR nyilvántartás dokumentumban, a fenyegetések értékelése a Kockázatelemzés dokumentumban került elkészítésre.

4.1.1. A területre kihelyezett kamerák

A területre kamerát kihelyezni és üzemeltetni csak a jelen szabályzatban foglaltak szerint, a kamera elhelyezési döntésének megfelelően lehet. A kamerákat tehát a szabályzat által meghatározott helyre lehet kihelyezni úgy, hogy a szabályzatban szereplő terület megfigyelésére legyen alkalmas.

A kamerák pontos kihelyezési helyéről a (2.2. pont szerinti) ellenőrző személyzet a megfigyelni szánt terület jól láthatósága figyelembevételével dönt. Indokolt esetben javaslatot tehet adott terület pontos megfigyelése érdekében több kamera elhelyezésére a Szervezet vezetője számára.

A területet igénybe vevő személyek tájékoztatása a térfigyelő rendszer működtetéséről

A kamerákat jól látható helyre kell kihelyezni. A kihelyezett kamerák üzemeltetésének tényéről minden megfigyelt helyen tájékoztatót kell kihelyezni.

A tájékoztatásnak tartalmaznia kell legalább:

- a képfelvévők elhelyezésének tényét,
- az adatkezelés rendjét.

A tájékoztatást úgy kell elhelyezni, hogy a területre belépni kívánó személyek számára a megfigyelés előtt láthatóvá váljon a tájékoztatás. A tájékoztatást szemmagasságban, jól látható helyen, illetve helyeken kell feltüntetni.

Az alkalmazott kamera típusa

A térfigyelő rendszerben a megfigyelés céljának megfelelő műszaki tanúsítvánnyal rendelkező kamerákat lehet alkalmazni.

4.1.2. Tájékoztatás

A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény 28. § (2) bekezdés c) pontja által előírtaknak megfelelően, az épületben megjeleni kívánó harmadik személyek részére a Szervezet figyelemfelhívó jelzést helyez el annak tényéről, hogy az adott területen elektronikus térfigyelő rendszer működik. A munkavállalók tájékoztatása a „SZABÁLYZAT A MUNKAHELYI TERÜLETI TÉRFÍGYELŐ KAMERA RENDSZER ÜZEMELTETÉSÉRE” szabályzatban rögzítettek szerint történik.

4.1.3. A központi helyiség

A területi térfigyelő kamera rendszer telephelyenkénti adatkezelő helyisége az Jászberényi V.V. Nonprofit Zrt. adott épületeinek erre a célra biztosított helyiségében található.

A kihelyezett kamerák által közvetített képek:

- folyamatos figyelemmel kísérésének lehetőségét monitor biztosítja,
- a képek rögzítése egy hátsó tároló egységre (winchester) vagy, bizonyos esetekben, SD kártyára történik.

4.1.4. A felvételek megtekintése

A Szervezet által alkalmazott térfigyelő rendszer közvetlen megfigyelésre (élőkép) használható, közvetlen megfigyelésre kizárólag a jelen szabályzat szerinti munkakörben foglalkoztatott munkatársaknak, és kizárólag a munkakörük ellátásához szükséges mértékben van joga. A képfelvételek megtekintésére és esetleges visszanezésére szolgáló monitort úgy kell elhelyezni, hogy a képfelvételek sugárzása alatt azokat a jogosultsági körön kívüli személyek ne láthassák.

4.2. A rendszer üzemeltetési rendje

4.2.1. A rendszer üzemeltetésének célja

A munkavállalók megfigyelése az Mt. 9. § és 11. § előírásai szerint valósulhat meg. Az üzemeltetés során be kell tartani az Infotv. 4. § előírásait.

A területi térfigyelő kamera rendszer üzemeltetésének elsődleges célja:

- a) az emberi élet, testi épség, személyi szabadság védelme,
- b) a veszélyes anyagok őrzése,
- c) az üzleti, fizetési, bank- és értékpapírtitok védelme,
- d) vagyonvédelem

A Szervezet az Szvtv. 26. § (1) bekezdése szerint járhat el a létesítményei őrzése során, kivéve, hogy a (2) bekezdés értelmében elektronikus megfigyelőrendszert közterületen ilyenkor sem alkalmazhat.

4.2.2. A rendszer tulajdonosa és üzemeltetője

A területi térfigyelő kamera rendszer a Jászberényi V.V. Nonprofit Zrt. tulajdona. A rendszer használatára, kezelésére, üzemeltetésére a Szervezet által meghatározott egység és személyzet jogosult.

4.2.3. A Térfigyelő területi térfigyelő kamera rendszer üzemeltetése

A térfigyelő területi térfigyelő kamera rendszer által közvetített képek megfigyelése

A térfigyelő területi térfigyelő kamera rendszer által közvetített képek esetenként megfigyelésre kerülnek

A térfigyelő területi térfigyelő kamera rendszer által közvetített képek megfigyelésének célja, hogy az ellenőrző személyzet áttekintést kapjon a megfigyelt területek állapotáról, helyzetéről, és indokolt esetben azonnali intézkedést tegyen, illetve kezdeményezzen.

A térfigyelő területi térfigyelő kamera rendszer képeinek rögzítése

A térfigyelő területi térfigyelő kamera rendszer képeinek rögzítése:

- folyamatosan - a nap 24 órájában - történik,
- folyamatosan - a nap 24 órájában - történik, de csak mozgás esetén kapcsol be a kamera.

A képek rögzítésének célja, hogy szükséges esetben bizonyítási eszközként felhasználhatók legyenek az egyes eljárásokban.

4.2.4. A rögzített felvételek visszánézése

A térfigyelő területi térfigyelő kamera rendszer rögzített képeinek visszánézése a visszánézésre okot adó esemény bekövetkezésekor történik meg. Eljárás: ld. 3. melléklet

A visszánézett felvételeken el kell különíteni:

- a rendkívüli eseményt tartalmazó, (azaz a felvételek adatkezelésére indokot, eljárás megindítására, illetve kezdeményezésére okot adó) felvételrészeket,
- a rendkívüli eseményt nem tartalmazó felvételektől.

Felvételek törlése: Ld. 5.5 Az adatkezelés időtartalma, az adatok törlése

4.2.5. Eljárás indítása, illetve kezdeményezése

A rendkívüli eseményt tartalmazó felvételek esetén a rögzített kép-, hang-, valamint kép- és hangfelvétel rögzítésétől számított két munkanapon belül a terület felügyelő köteles:

- a feladatkörébe tartozó eljárást megindítani,
- a más szerv vagy hatóság (pl. rendőrség) hatáskörébe tartozó eljárások esetén az eljárás megindítását kezdeményezni.

5. A területi térfigyelő kamera rendszerrel kapcsolatos adatkezelés

5.1. A területi térfigyelő kamera rendszer által rögzített felvételek, mint személyes adatok

A területi térfigyelő kamera rendszerben rögzített felvételek személyes adatnak minősülnek, ezért érvényesíteni kell az információs törvényben szülő törvényben meghatározott, valamint jelen szabályzatban meghatározott adatkezelési szabályokat.

5.2. Az adatkezelés alapelvei

Az adatkezelés főbb alapelvei:

- személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető,
- az adatkezelés során az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie,
- személyes adat csak a cél megvalósulásához szükséges mértékben kezelhető.

Az ellenőrzésre jogosultak részéről a személyes adat kezelésének célja:

- a) az emberi élet, testi épség, személyi szabadság védelme,
- b) a veszélyes anyagok őrzése,
- c) az üzleti, fizetési, bank- és értékpapírtitok védelme,
- d) vagyonvédelem.

5.3. Az adatkezelés jogalapja

A szervezet a megfigyelést a GDPR 6. cikk 1. bekezdés f) pontja alapján, jogos érdekéből fakadóan végzi. Alkalmazott vagyonőri szolgálat esetén az ellenőrzésre jogosultak adatkezelésének jogalapját az Szvtv. 26. § (1) bekezdése, illetve a 30. §-a határozza meg.

5.4. Az adatkezelés korlátai

A területi térfigyelő kamera által rögzített felvételeket, mint személyes adatokat a képfelvétellel érintett területen:

- elkövetett bűncselekmény miatt indult eljárásban,
- elkövetett szabálysértés miatt indult eljárásban,
- a felvételen szereplő személy által, jogainak gyakorlása érdekében indított eljárásban használható fel.

A területi térfigyelő kamera által rögzített felvételeket bizonyítási eszközként ki kell adni:

- a bírósági vagy más hatósági eljárásban jogosult szerv kérésére, illetve
- közigazgatási hatósági eljárásban az eljáró hatóság megkeresésére (belföldi jogsegély keretében), ha a megkereső szerv a kérelmét jogszabálynak megfelelően indokolta.

Az indokolás akkor megfelelő, ha az tartalmazza:

- a megkereső szerv jogosultságát megalapozó alapvető jogszabályi hivatkozást,
- az eljárás tárgyát,
- az eljárás ügyiratszámát,
- a rögzített felvétellel bizonyítandó tény.

A megkeresést meg kell tagadni, ha:

- a megkeresés indoklása nem megfelelő,
- ha a rögzített kép-, hang-, valamint kép- és hangfelvétel a megkeresésben meghatározott tény bizonyítására alkalmatlan.

A kiadott felvételeket csak abban az esetben kell titkosítani (jellemzően ha magánszemélyek kérelmére kerül a felvétel átadásra), ha fennáll a kockázata, hogy harmadik személyek is hozzáférhetnek azokhoz illetéktlenül. Ebben az esetben a titkosító kódot (jelszót) a felvételtől elkülönülten, eltérő kommunikációs csatornán kell eljuttatni.

5.5. Az adatkezelés időtartalma, az adatok törlése

Az Infotv. alapján az adatkezelés során személyes adat csak a cél megvalósulásához szükséges ideig kezelhető.

A rendkívüli eseményeket nem tartalmazó felvételek adatkezelési időtartama

A rendkívüli eseményeket nem tartalmazó felvételeket a rögzítést követő 15 napig (állatkert esetében 30 napig) kezelhetőek, azt követően haladéktalanul törölni kell, kivéve az SD kártyákat tartalmazó kamerákat, amelyek mozgás érzékelővel rendelkeznek, így a tárhely kapacitása és a bekapcsolási események együttesen határozzák meg a megőrzés időtartamát.

A rendkívüli eseményeket tartalmazó felvételek adatkezelésének időtartalma

A rendkívüli eseményeket tartalmazó felvételek adatkezelési időpontja nem haladhatja meg a 15 napot (állatkert esetében 30 napot). Az adatkezelés akkor tarthat tovább a rögzítést követő 15 napnál (állatkert esetében 30 napnál), ha a felügyelet által kezdeményezett eljárás során az eljárás megindítására jogosult az eljárás megindításának tényéről a rögzítést követő 15 napon belül a felügyeletet tájékoztatta.

Ha az eljárást lefolytató szerv részére, vagy magánszemély számára a jogainak gyakorlása érdekében indított eljárásban az adat továbbítása megtörtént, az adatokat törölni kell.

Kérelemre az adatkezelés időtartamának meghosszabbítása

Az, akinek jogát vagy jogos érdekét a kép-, hang-, vagy a kép- és hangfelvétel, illetve más személyes adatának rögzítése érinti, a kép-, hang-, valamint kép- és hangfelvétel, illetve más személyes adat rögzítésétől számított tizenöt napon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje. Bíróság vagy más hatóság megkeresésére a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre attól számított 30 napon belül, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell. A rögzített felvételen szereplő személy részére az adattovábbításról adott tájékoztatás költségmentes.

Tárolók törlése

A tárolóeszközök tartalmát (belső SD kártyák, kimentett felvételeket tartalmazó adathordozók) az eszközök selejtezése, megsemmisítése, újrahasznosítás esetén a Szervezet "Adathordozók védelmére vonatkozó szabályzat"-ban foglaltaknak megfelelően kell elvégezni.

5.6. Betekintési jog

Az ellenőrzésre jogosultak részéről biztosítani kell az érintett magánszemélyek számára, hogy a felvételen szereplő személy - az adatkezelésre rendelkezésre álló időtartama alatt, jellemzően a rögzített kép-, hang-, valamint kép- és hangfelvétel készítésétől számított 15 napon belül, piac esetében szintén 15 napon belül, - megtekinthesse a róla készült felvételt. Az érintett a jogait az Infotv. 14-19. §-ban foglaltak szerint gyakorolhatja. Eljárás: ld. 3. melléklet

Idegenek jelenlétében a felvételek visszanezését meg kell szakítani, ha a visszanezett adatok idegen általi megismerhetőségét más módon nem lehet kizárni.

6. Adatbiztonság

A szervezet területi térfigyelő kamera rendszerének napi üzemeltetését a szervezet megbízásából külső szolgáltató végzi, amely alvállalkozóként, adatfeldolgozóként, látja el a rendszergazdai és műszaki üzemeltetési feladatokat. A külső szolgáltató a szervezettel kötött szerződés alapján jogosult a rendszer működtetésére, karbantartására, hibaelhárítására és – a szerződésben meghatározott keretek között – bizonyos konfigurációs beállítások elvégzésére. A területi térfigyelő kamera rendszer feletti rendelkezési jog, az adatkezelési döntések, valamint az információbiztonsági és adatvédelmi felelősség továbbra is a Szervezetenél marad, mint adatkezelő és mint a rendszer üzemeltetéséért felelős szervezet. A külső szolgáltató kizárólag a szervezet Gazdasági igazgatója írásos utasításai alapján és azokkal összhangban végezhet tevékenységet.

6.1. Szervezési intézkedések

6.1.1. Jogosultságok

A területi térfigyelő kamera rendszer használatát, felépítését a vezérigazgató hagyja jóvá. A területi térfigyelő kamera rendszer által rögzített felvételek kezelését a rendszerben kizárólag meghatározott személyek, az ellenőrzésre jogosultak végezhetik, hitelesítést követően:

- elsődlegesen az IT rendszergazda (admin), azaz Járvás Róbert üzemeltető alvállalkozó (teljes rendszer kezelési jogosultság),
- felhasználók (megtekinzési, megfigyelési, letöltési jogosultság):
 - o Városi strand és termálfürdő: közjóléti ágazatvezető – Baranyiné Hallgat Magdolna

- Bercsényi úti Sportcsarnok: üzleti asszisztens – Teleki Zoltán
- Hulladékudvar: kommunális ágazatvezető – Tóth Endre
- Jákóhalmi úti telep: portaszolgálat

A fenti kijelölt felhasználók jogosultak:

- a kamerák által közvetített képek megfigyelésére, valamint
- a kamera rendszer által rögzített képek visszánézésére,
- a rögzített felvételek, illetve felvételrészek elkülönítésére rendkívüli és nem rendkívüli események szerint.

Az admin felhasználó a felhasználók jogain túl jogosult:

- az adat kimentésére (külön engedéllyel),
- az adat továbbításra (külön engedéllyel),
- az adattörlésre (külön engedéllyel),
- a rendszerkezelő felületre belépésre,
- a naplózási és a rendszeres ellenőrzési kötelezettségek elvégzésére,
- a rendszer beállításainak, konfigurációjának vizsgálatára, karbantartására, módosítására (külön engedéllyel).

A jogosultságok és a rendszer szükségességének felülvizsgálata legalább évente vagy szervezeti változás esetén történik meg.

Az ellenőrzésre jogosultak részéről biztosítani kell az érintettek személyes adatainak védelmét. A védelemnek ki kell terjednie a magántitoknak és magánélet körülményeire, arra, hogy ezek illetéktelen személy tudomására ne jussanak.

Az adatokat védeni kell különösen:

- a jogosulatlan hozzáférés,
- a jogosulatlan megváltoztatás,
- a jogtalan továbbítás,
- a jogtalan nyilvánosságra hozatal,
- jogszerűtlen törlés vagy megsemmisítés, valamint
- a véletlen megsemmisülés és sérülés ellen.

A rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot csak az a személy- és vagyónvédelmi tevékenységet végző személy jogosult megismerni, akinek ez a szerződésből fakadó kötelezettségei érvényesítéséhez szükséges, és a jogsértő cselekmény megelőzése vagy megszakítása érdekében mellőzhetetlen. A rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint személyes adatot kezelő, vagy egyéb okból annak megismerésére jogosult személy- és vagyónvédelmi tevékenységet végző személy nevét, az adatok megismerésének okát és idejét jegyzőkönyvben kell rögzíteni.

6.1.2. Üzembiztonság

A rögzítőeszközök zárt helységben, azon belül is zárt rack szekrényben kerültek elhelyezésre, amelyekhez kulccsal az arra jogosultak tudnak belépni, az eszközökhöz fizikailag csak az arra jogosult (admin felhasználó) fér hozzá kulccsal és az eszközökbe csak arra jogosultak csak a jelszósabályok szerint kialakított jelszóval tudnak belépni. A rendszer kiszolgálásra alkalmas eszközök, és egyéb adathordozók - a jogszerű adattovábbítás kivételével - a helyiségből ki nem vihetőek. Alapvető biztonsági események, amelyek ellenőrzést igényelnek: kamera meghibásodása, engedély nélküli belépés, hozzáférés, illetéktelen hozzáférés a kamera felvételeihez, felvételek illetéktelen törlése. Az eszközök dokumentációját a rendszergazda tárolja, hiányzó dokumentáció esetén helyettesítő dokumentum bekérése szükséges, illetve belső vizsgálat indítása a hiányosságok javítása céljából.

Az informatikai eszközök karbantartása esetén is gondoskodni kell az adatvédelmi előírások betartásáról. Karbantartást, javítást csak az arra jogosult jelenlétében lehet végezni, ez elsődlegesen az admin felhasználó. A területi térfigyelő kamera rendszer működésének megszüntetését a vezérigazgató utasítása szerint a megfigyelési célok megszűnése, teljesülése, a megfigyelésre vonatkozó kockázat kritikussá válása vagy a telephely megszűnése esetén végzi el a rendszergazda.

Rendkívüli ellenőrzés

Rendkívüli ellenőrzést abban az esetben kell elvégezni, amennyiben az eszköz hibát jelez (naplóbejegyzés hibája esetén hangjelzést ad), megsérül vagy nem működik. Az ellenőrzés és hibajavítás (újraindítás, javítás) az admin felhasználó feladata. A meghibásodás, sérülés, hiba tapasztalatai alapján az admin felhasználó javaslatot tesz a Gazdasági igazgatónak a rendszerek kockázatainak felülvizsgálatára, amennyiben az indokolt és szükséges.

Negyedéves ellenőrzés

Az admin felhasználó, legalább negyedévente ellenőrzi a rendszer üzemelését (minden év végén a negyedéves ellenőrzés éves ellenőrzést is magába foglal ld. lent), ennek során ellenőrizni kell a rendszer és elemeinek fizikai állapotát, konfigurációját, kapcsolatait, szoftvereit, beállításait, a rendszer jogosulatlan használatát, a rendelkezésre álló memória állapotát, telítettségét, naplóbejegyzéseit. Ellenőrizni kell továbbá a kamerák és rögzítők fizikai védettségét, sértetlenségét, a szabotázs jeleit, a tápellátás folytonosságát, valamint a kültéri eszközök környezeti hatásokkal szembeni állapotát. Vizsgálni kell az alkalmazott, sérülékeny szoftverek, firmware-ek verzióit és naprakészségét, szükség esetén frissítésüket, elvégzi a patch managementet és a gyártói oldalakat ellenőrzi a lehetséges javításokat, frissítéseket, új verziókat (ezeket az ellenőrzést követően a Patch- és sérülékenységkezelési szabályzatban meghatározott kritériumoknak és időtartamoknak megfelelően telepíteni kell, biztonsági tesztelést követően). Át kell tekinteni a rendszer felhasználói jogosultságkezelését, az inaktív vagy jogosulatlan felhasználói fiókok törlését, valamint a naplózási események meglétét, épségét és telítettségi állapotát. Ellenőrizni szükséges a videofelvételekhez kapcsolódó adatmegőrzési szabályok betartását, a visszakereshetőség és a törlődési ciklusok működését. A

hálózati beállítások, IP-címek konfigurációi szintén vizsgálatra szorulnak, különös tekintettel a kamerák közötti és a külső kapcsolatokat érintő változásokra. Végre kell hajtani kameránként teszt-rögzítést és riasztási funkcióellenőrzést, valamint az automatikus értesítések (pl. kiesés, mozgás, rögzítésleállítás) működésének vizsgálatát. Az ellenőrzés során tesztelni kell a naplóbejegyzések rögzítését és a sikertelen belépésekre vonatkozó beállításokat is.

A negyedéves ellenőrzést minden esetben dokumentált módon, írásban kell rögzíteni, különös tekintettel az észlelt hibákra, eltérésekre, javítási javaslatokra és azok felelőseire.

Az ellenőrzésekről naplóbejegyzést kell készíteni (ellenőrzött rendszer helyszíne, ellenőrző személye, ellenőrzés dátuma, megjegyzések/hibák), amit a Gazdasági igazgató jóváhagyásával lát el.

Éves ellenőrzés

Az admin felhasználó évente egy alkalommal biztonsági ellenőrzést köteles végezni a kamerák kapcsán, a vonatkozó terv és eljárásrend előírásainak megfelelően (ld. melléklet). Az éves ellenőrzés során a jelen szabályzat, mint rendszerbiztonsági terv, felülvizsgálatát is végre kell hajtani. Az ellenőrzésekről jegyzőkönyvet kell készíteni, amit a Gazdasági igazgató jóváhagyásával lát el.

6.1.3. Adattovábbítás

Adatot továbbítani csak a jelen szabályzatban - és jogszabályban - meghatározott esetekben lehet. Az adattovábbítás az eljárásra jogosult szerv, hatóság képviselője által biztosított adat hordozó eszközre történik.

6.2. Technikai intézkedések és beállítások

Szünetmentes áramforrás

Lehetőség szerint szünetmentes áramforrás biztosításával kell gondoskodni arról, hogy a rendszer folyamatosan működni tudjon, illetve áram kimaradás miatt üzemzavar ne következzen be.

Informatikai védelem

Az adatállományok kezelését úgy kell megszervezni, hogy részleges vagy teljes megsemmisülés esetén tartalmuk rekonstruálható legyen. Az eredeti adatállományokról legalább egy biztonsági mentést kell készíteni, hogy az egyik megsemmisülése, sérülése esetén az eredeti adatok továbbra is rendelkezésre álljanak.

Adathordozó azonosítása

A rendszerben csak nyilvántartásba vett adathordozót lehet használni, hogy a kezelt adatok fellelési helye, megsemmisítése nyomon követhető legyen. Az adattovábbítást kivéve adathordozóként csak a számítógéptől el nem különülő tárhelyet lehet használni.

Területi térfigyelő kamera rendszer lényeges működési képességei

A területi térfigyelő kamera rendszer alapvető, fenntartandó működési képességei az alábbiak:

- Folyamatos képalkotás és rögzítés a kijelölt területeken.
- A felvételek biztonságos tárolása és visszakeresése a meghatározott megőrzési időn belül.
- Az eszközök működőképességének ellenőrzése, beleértve a fizikai sértetlenséget és a tápellátást.
- A felhasználók részére biztosított hozzáférés a munkaköri jogosultságok alapján.
- A naplók és rendszeresemények rögzítése, amelyek a működés ellenőrizhetőségét biztosítják.
- A rendszer biztonságos helyi kezelése, távoli elérés nélkül.

Tiltott vagy korlátozott funkciók

A területi térfigyelő kamera rendszerben tilos vagy korlátozott minden olyan funkció, amely a szükséges üzemi működést nem szolgálja, különösen:

- Távoli hozzáférés biztosítása a rögzítőhöz vagy kamerákhoz.
- Felesleges funkciók és menüpontok aktiválása, amelyek a rendszer működésében nem töltenek be üzemi szerepet.
- Nem engedélyezett adminisztrátori jogosultságok létrehozása vagy módosítása.
- Automatikus továbbítás, streaming, vagy hálózati megosztások tiltása, amelyek a rendszer működéséhez nem szükségesek.

Tiltott vagy korlátozott portok

A területi térfigyelő kamera rendszer zárt fizikai struktúrában működik, hálózati kapcsolattal nem rendelkezik.

Ennek megfelelően, minden hálózati kommunikációt igénylő port használata tiltott, kivéve a gyártó által biztosított, kizárólag helyi (kábeles) eszköz–eszköz kommunikációhoz szükséges kapcsolatokat.

Tiltott vagy korlátozott protokollok

A rendszer működése nem igényel hálózati protokollokat. Ezért minden olyan protokoll használata tiltott, amely hálózati, internetes vagy távoli kommunikációt tesz lehetővé. A kamerák és a rögzítő közötti kommunikáció kizárólag a gyártó által definiált helyi, közvetlen fizikai kapcsolaton valósulhat meg.

Tiltott vagy korlátozott szoftverek

A területi térfigyelő kamera rendszerben nem telepíthető semmilyen külső szoftver, nem futtatható harmadik féltől származó alkalmazás, mivel a rendszer kizárólag a gyártó által biztosított rögzítő- és kezelői szoftver segítségével üzemel.

Tiltott vagy korlátozott szolgáltatások

A területi térfigyelő kamera rendszerben tiltott minden olyan szolgáltatás, amely hálózati kommunikációt igényel, a rendszer működését nem szolgálja, jogosulatlan hozzáférés vagy adatmozgás kockázatát növeli.

Különösen tiltott a távoli menedzsment, internetkapcsolat, felhőszolgáltatások igénybevétele, külső továbbítás vagy megosztás (kivéve a minősített eseteket, amelyek a gazdasági igazgató engedélyéhez kötöttek).

6.3. Információcsere

A területi térfigyelő kamera rendszer elemei – a kamerák és a rögzítő – zárt rendszerben, közvetlen fizikai kábellel összekötve működnek, hálózati kapcsolódás nélkül. A két eszköz között így is folyamatos információcsere történik, mivel a kamera a videójelet és a kapcsolódó metaadatokat a rögzítő számára továbbítja. A szervezet az alábbiak szerint szabályozza ezt az információcsere:

A szervezet jóváhagyja és szabályozza a kamerák és a rögzítő közötti információcsere. A kapcsolat a szervezet biztonsági és működési követelményei alapján létrehozott, kizárólag belső célú adatátviteli csatorna, amelyet a vonatkozó szabályzatoknak megfelelően kell üzemeltetni.

A kapcsolatra vonatkozó megállapodás rögzíti:

- a fizikai interfész jellemzőit (pl. UTP/koaxiális kábel, közvetlen pont-pont kapcsolat),
- az alkalmazott védelmi intézkedéseket (fizikai védelem, szabotázs elleni védelem, kábelvezetési követelmények),
- a felelősségi köröket (rendszergazda, mint üzemeltető),
- valamint a kamerák által továbbított adatok – videójel, metaadatok – kezelésének és védelmének módját.

A szervezet rendszeres időközönként (ld. 6.1.2) felülvizsgálja a kapcsolatot és az információcsere-megállapodásban rögzített feltételek aktualitását, különös tekintettel a fizikai sértetlenségre, a kábelezés állapotára, az eszközök védelmére és az adatkezelési követelmények betartására.

Ezzel a dokumentált folyamattal a szervezet biztosítja, hogy a kamerák és a rögzítő közötti, hálózatot nem érintő, kizárólag fizikai adatkábelen történő adatmozgás is ellenőrzött, szabályozott és nyomon követhető információcsere minősüljön, összhangban a vonatkozó biztonsági követelményekkel.

6.4. Kockázatmonitorozás és folyamatos felügyelet

A szervezet biztosítja, hogy a területi térfigyelő kamera rendszerrel kapcsolatos kockázatmonitorozás a folyamatos felügyeleti stratégia szerves része legyen. A felügyelet célja annak ellenőrzése, hogy a rendszer a meghatározott biztonsági, működési és adatkezelési követelményeknek folyamatosan megfeleljen, és hogy a biztonsági helyzetben bekövetkező változások időben azonosíthatók legyenek. A kockázatmonitorozási folyamat az alábbi elemeket tartalmazza.

6.4.1. A hatékonyság ellenőrzése

A szervezet rendszeresen (ld. 6.1.2) vizsgálja a területi térfigyelő kamera rendszer biztonsági és működési intézkedéseinek hatékonyságát, különös tekintettel a fizikai védelemre, a hozzáférések szabályozására, a naplózás állapotára, a riasztási funkciók működésére, valamint a felvételek védelmére. A vizsgálat célja annak megállapítása, hogy az alkalmazott védelmi intézkedések továbbra is alkalmasak-e a feltárt kockázatok csökkentésére.

6.4.2. A megfelelés ellenőrzése

A szervezet értékeli, hogy a területi térfigyelő kamera rendszer üzemeltetése megfelel-e a vonatkozó jogszabályi, adatkezelési, információbiztonsági és belső szabályozási követelményeknek. A megfeleléseellenőrzés kiterjed a jogosultságkezelésre, az adatmegőrzési előírásokra, a kezelési naplókra, az adatbiztonsági intézkedések meglétére és a technikai beállítások szabályszerűségére.

6.4.3. A változások nyomon követése

A szervezet figyelemmel kíséri a területi térfigyelő kamera rendszer működését érintő technikai, fizikai vagy szervezeti változásokat, beleértve a kamerák cseréjét, áthelyezését, szoftver- vagy firmware-frissítéseket, konfigurációmódosításokat és hálózati vagy adatkezelési változásokat. A változások nyomon követése biztosítja, hogy minden módosítás után újraértékelésre kerüljenek a kapcsolódó kockázatok, és szükség esetén módosuljanak a védelmi intézkedések.

6.5. Változáskezelés és előzetes információbiztonsági hatásvizsgálat

A szervezet biztosítja, hogy a területi térfigyelő kamera rendszert érintő bármely tervezett változtatás bevezetése előtt elvégezze a módosítás információbiztonsági hatásainak vizsgálatát. A hatásvizsgálat célja annak megállapítása, hogy a tervezett változtatás milyen kockázatot jelent a rendszer rendelkezésre állására, sértetlenségére, bizalmasságára és jogszabályi megfelelésére.

A tervezett változtatások körébe tartozik különösen:

- új kamera telepítése vagy meglévő kamera áthelyezése;
- kamera vagy rögzítő csere;
- szoftver- és firmware-frissítések;
- a rögzítő vagy a kamerák konfigurációjának módosítása;
- kábelezési vagy fizikai infrastruktúrában történő változtatás;
- jogosultságok, hozzáférések vagy kezelőfelületek megváltoztatása;
- a rendszer működéséhez szükséges technikai feltételek módosítása.

A változtatást megelőző információbiztonsági hatásvizsgálat során a szervezet értékeli:

- A változtatás biztonsági kockázatait – ideértve a sérülékenységek, jogosulatlan hozzáférések, adatvesztési vagy működéskiesési veszélyeket.
- A változtatás megfelelésre gyakorolt hatását – az adatvédelmi, információbiztonsági és jogszabályi követelmények teljesülése szempontjából.
- A működés folytonosságára gyakorolt hatást – annak vizsgálatával, hogy a módosítás érinti-e a felvételkedzítést, visszanzéhetőséget vagy a bizonyítékként felhasználhatóságot.
- Az érintett rendszerelemek biztonsági kontrolljainak szükséges erősítését vagy módosítását.

A változás csak akkor vezethető be, ha:

- a hatásvizsgálat lezárult,
- a szükséges kockázatsökkentő intézkedéseket meghatározták,

- a változtatást a szervezet vezetője vagy az információbiztonságért felelős személy jóváhagyta.

A szervezet minden változtatást dokumentál, és a kapcsolódó iratokat a területi térfigyelő kamera rendszer üzemeltetési dokumentációjának részeként megőrzi. A változáskezelési dokumentáció a későbbi ellenőrzések, auditok és biztonsági vizsgálatok során felhasználható.

6.6. Egységes biztonsági konfigurációk

6.6.1. Egységes biztonsági konfigurációk

A szervezet a területi térfigyelő területi térfigyelő kamera rendszer minden rendszerelemére egységes biztonsági konfigurációkat határoz meg, amelyek célja a rendszerelemek biztonságos kiindulási állapotának rögzítése, az eltérések felismerhetősége és a konfigurációk következetes dokumentálhatósága. A konfigurációk a rendszer üzemeltetési követelményeivel összhangban a legkorlátozottabb, biztonságos üzemmódot tükrözik.

6.6.2. Konfigurációs alapbeállítások (baseline)

A szervezet az alábbi, dokumentált konfigurációs alapbeállításokat (baseline) alkalmazza a kamerák és rögzítőegységek esetében:

Kamerák minimális biztonsági konfigurációja

- egyedi, erős jelszó alkalmazása (kis és nagy betű, különleges karakter, szám, legalább 8 karakter hosszúságú);
- felesleges szolgáltatások és protokollok letiltása (ha van);
- pontos idő- és dátumszinkron;
- rögzítővel biztonságos kommunikáció alkalmazása, ha a gyártó biztosítja;
- firmware naprakész állapotának fenntartása;
- hozzáférési felületek minimalizálása;
- a kezelői felület elérése csak jóváhagyott felhasználó számára biztosított.

Rögzítőegységek minimális biztonsági konfigurációja

- egyedi adminisztrátori jelszó;
- felhasználói jogosultsági szintek elkülönítése;
- naplózás bekapcsolása és naplók megőrzése;
- jelszócsere kötelezővé tétele (ha támogatott);
- tárolási idő és törlési ciklusok rögzítése és védelme;
- felesleges szolgáltatások letiltása;
- távoli hozzáférés tiltása (a rendszer hálózattól való elszigeteltsége miatt).

6.6.3. Konfigurációs dokumentáció és verziókövetés

A szervezet minden rendszerelem aktuális konfigurációját dokumentálja, és a változásokat nyomon követhető módon rögzíti.

A konfigurációs állapot vizsgálata része:

- a negyedéves ellenőrzéseknek (naplózás, verziók, beállítások ellenőrzése) ,
- valamint az éves biztonsági értékelésnek, amelyben vizsgálni kell, hogy a konfiguráció megfelel-e az egységes baseline elvárásoknak.

A szervezet biztosítja, hogy minden dokumentált változtatás a vonatkozó szabályzatok szerinti változáskezelési eljárás alapján történjen.

6.6.4 Az eltérések jóváhagyását szükségessé tevő működési követelmények

A szervezet meghatározza azokat a működési körülményeket, amelyek indokoltá tehetik az egységes biztonsági konfigurációktól való eltérést. Eltérés csak akkor engedélyezhető, ha az a rendszer működőképességének fenntartása, hibaelhárítása vagy üzemfolytonossága érdekében szükséges.

Eltérés különösen az alábbi esetekben engedélyezhető:

1. Gyártói korlát vagy kompatibilitási probléma, amely miatt a baseline-beállítás nem alkalmazható.
2. Hibás, sérült vagy meghibásodott eszköz ideiglenes üzembe helyezése, amely a biztonsági konfigurációktól való átmeneti eltérést tesz szükségessé.
3. Üzemfolytonossági ok, amikor a konfigurációs előírások szerinti beállítás fennakadás nélkül nem biztosítható.
4. Biztonsági frissítések vagy firmware-módosítások átmeneti inkompatibilitása, amely miatt az eredeti konfiguráció ideiglenesen nem állítható vissza.

Minden eltérést dokumentálni kell, és az arra jogosult jóváhagyó személy (adminisztratív felelős vagy gazdasági igazgató) engedélye szükséges. Az eltérést a következő rendszeres felülvizsgálat során újraértékelik.

6.6.5. Eltérések azonosítása és jóváhagyása

A dokumentumtartalom alapján a területi térfigyelő kamera rendszerre vonatkozóan előírt, rendszeres ellenőrzések során fel kell tárni:

- az egységes konfigurációtól való eltéréseket,
- a hibás vagy nem engedélyezett beállításokat,
- a frissítések, firmware állapotának eltéréseit.

Az észlelt eltéréseket dokumentálni kell, és az erre jogosult személy jóváhagyásával kell kezelni (admin felhasználó, gazdasági igazgató jóváhagyásával).

6.6.6. Konfigurációs ellenőrzések rendszeressége

Ellenőrzések:

- negyedéves rendszerellenőrzés, amely kiterjed beállításokra, hibákra, naplókra, verziókra;
- éves technikai megfelelőségi értékelés, amely vizsgálja az egységes baseline-nal való egyezést.

7. Nyilvántartás vezetési kötelezettség

A területi térfigyelő területi térfigyelő kamera rendszer működtetéséhez kapcsolódva nyilvántartást kell vezetni:

- a kihelyezett kamerákról és az általuk megfigyelt területről (kamera nyilvántartás),
- a rendszer állapotának rendszeres ellenőrzéséről (üzemeltetési napló),
- a rendszerben végzett megfigyelésekről (megfigyelési napló),
- a rendszerben rögzített felvételek visszanezéséről, és kimentéséről (visszanezési napló),
- a rendszerben a felvételek tárolására használt adathordozókról, (adathordozó nyilvántartás),
- a rendszerben tárolt adatokról másolatkészítésről (adat másolati napló),
- az adattovábbításról, (adattovábbítási napló)
- a felvételek megsemmisítéséről,
- az adatvédelmi incidensről.

7.1. Kamera nyilvántartás

A kamera nyilvántartásnak tartalmaznia kell legalább:

A kamerák egyedi azonosító adatai:

- kamera sorszáma,
- gyártó és típus,
- egyedi eszközazonosító (ha elérhető),
- telepítési hely pontos megjelölése,
- annak rögzítése, hogy a kamera vezetékes (nem Wi-Fi) technológiával működik.

A rögzítőegységek azonosító adatai:

- eszköz sorszáma,
- gyártó, típus,
- egyedi eszközazonosító,
- a rögzítő fizikai elhelyezése.

A rögzítőegységeken futó szoftverek és firmware-ek adatai:

- szoftver/firmware neve,
- verziószáma,
- verzió kiadásának dátuma,
- üzemeltetőtől kapott információ arról, hogy a verzió gyártói támogatása érvényben van-e.

A kamerák firmware-adatai:

- firmware verziószáma,
- telepítés vagy utolsó frissítés időpontja,
- gyártói támogatási státusz (amennyiben elérhető az üzemeltetőtől).

Az összes rendszerelem esetében (megjegyzés rovatban):

- a támogatás megszűnése vagy a szoftver/firmware elavultsága esetén az ebből eredő kockázatok feljegyzése,
- a szükséges frissítési vagy csereintézkedések rögzítése.

7.2. Üzemeltetési napló

A rendszer működtetése során a rendszer állapotának rendszeres ellenőrzéséről üzemeltetési naplót kell vezetni. Az üzemeltetési napló tartalmazza a rendszer állapot ellenőrzésre vonatkozó adatokat:

- az ellenőrzés pontos időpontját,
- a rendszer egyes elemeinek állapotára vonatkozó megjegyzést,
- a rendszer nem megfelelő üzemelése esetén a tett intézkedést,
- az ellenőrzést végző személy nevét,

7.3. Megfigyelési napló

A térfigyelő kamararendszer által közvetített felvételek megfigyelése esetén a megfigyelésre vonatkozó adatokat a megfigyelési naplóban kell rögzíteni.

A megfigyelési naplónak tartalmaznia kell:

- a megfigyelés napját,
- a megfigyelés kezdő és befejező időpontját,
- a bekövetkezett rendkívül eseményeket,
- a kezdeményezett intézkedéseket,
- a megfigyelő nevét.

7.4. Visszanézési napló

A térfigyelő kamararendszer által rögzített felvételek visszánézése esetén a visszánézésre, valamint a rendkívüli események képrészleteinek kimentésére vonatkozó adatokat naplóban kell rögzíteni.

A visszánézési naplónak tartalmaznia kell:

- a visszánézés napját,
- a visszánézett felvételek azonosításhoz szükséges adatokat: kamera szám, a rögzített kép-, hang-, valamint kép- és hangfelvétel rögzítés kezdő és befejező időpontját,
- a bekövetkezett rendkívül eseményeket,
- a rendkívüli eseményeket tartalmazó felvételrészek kimentésének adatai (mentés helye)
- a kezdeményezett intézkedéseket,
- a visszánéző nevét.

7.5. Az adathordozók nyilvántartása

Az adathordozó nyilvántartásnak tartalmaznia kell:

- a felhasznált, alkalmazott adathordozó azonosító adatait,
- az adathordozó adat rögzítésre történő használatának kezdő és befejező időpontját,

- az alkalmazást követően az adathordozó tárolási helyét,
- az adathordozó megsemmisítésére vonatkozó adatokat.

7.6. Adat másolási napló

Az adatmásolási naplónak tartalmaznia kell a rögzített felvételekről, rögzített kép-, hang-, valamint kép- és hangfelvétel részekről készített:

- másolat készítés időpontját,
- másolt rögzített kép-, hang-, valamint kép- és hangfelvétel azonosító adatait,
- másolat készítésének okát,
- másolat adathordozójának azonosítóját, a tárolás helyét,
- a másolatot készítő nevét.

7.7. Adattovábbítási napló

Az adattovábbítási nyilvántartást évenként kell vezetni, és a nyilvántartást 5 évig meg kell őrizni.

A nyilvántartásnak tartalmaznia kell, hogy:

- mikor történt az adattovábbítás,
- a felvételeket kinek, mely szervnek, hatóságnak, magánszemélynek továbbították,
- milyen célból került sor az adattovábbításra,
- mi volt az adattovábbítás jogalapja,
- a felvételek titkosítottan kerültek-e továbbításra.

7.8. Felvételek megsemmisítésének nyilvántartása

A felvételek megsemmisítéséről nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell:

- a megsemmisítés időpontját,
- a megsemmisített adatok azonosításához szükséges adatokat, /pl.: kamera szám, illetve számok, a rögzített felvételek időpontja (tól-ig) /,
- a megsemmisítés okát, (15 napon belüli, illetve egyéb)
- a megsemmisítés módját,
- a megsemmisítést végző nevét.

7.9. Incidens nyilvántartás

A nyilvántartásnak tartalmaznia kell:

- az incidenssel érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az incidens körülményeit,
- az incidens hatásait,
- az incidens elhárítására megtett intézkedéseket,

- egyéb jogszabályban meghatározott adatokat.

8. Feladat- és hatáskörök

Adatkezelési feladat-és hatásköröket gyakorol:

- a Szervezet vezetője vagy megbízottja.

8.1. Az ellenőrző személyzet vezetőjének adatkezelési feladat- és hatásköre

A Gazdasági igazgató adatkezelési feladata, hogy:

- a jelen szabályzatot kidolgozza,
- jelen szabályzatot változás esetén felülvizsgálja,
- a feladatok ellátásra kijelölje a feladatok ellátásáért felelős személyeket, a feladat elvégzéséről folyamatos tájékoztatást kérjen.

8.2. A terület-felügyelő adatkezelési feladat- és hatásköre

Az admin felhasználó adatkezelési feladata:

- a meghatározó belső szabályzatban rögzített szabályok betartása,
- a nyilvántartási feladatok elvégzése.

8.3. Beállítások kezelése, admin felhasználó feladatai

A szervezet a jelen dokumentumban megadott paramétereket, mint, egységes biztonsági konfigurációkat határozza meg a területi térfigyelő kamera rendszer minden rendszerelemére vonatkozóan annak érdekében, hogy a rendszer működése megfeleljen az információbiztonsági követelményeknek, és a konfigurációs beállítások kezelése, dokumentálása és ellenőrzése átlátható és auditálható legyen. Az egységes biztonsági konfigurációk célja:

- a rendszerelemek biztonságos kiindulási beállításainak meghatározása;
- az eltérések felismerhetőségének és vizsgálhatóságának biztosítása;
- a hibás vagy nem engedélyezett beállítások megelőzése;
- a konfigurációk következetes dokumentálása és felülvizsgálhatósága.

Alapértelmezett biztonsági követelmények rendszerelem-kategóriánként:

A kamerák konfigurációjának minimális biztonsági követelményei:

- egyedi, erős jelszó alkalmazása;
- felesleges szolgáltatások és protokollok letiltása (ha van);
- helyes dátum és idősinkron biztosítása;
- rögzítővel való titkosított vagy gyártói biztonsági csatornán történő kommunikáció (ha elérhető);
- firmware naprakész állapotának biztosítása;
- hozzáférési felületek korlátozása a szükséges minimumra;

- a kezelői felülethez való hozzáférés csak jóváhagyott felhasználó számára.

A rögzítőegységek konfigurációjának minimális biztonsági követelményei:

- egyedi adminisztrátori jelszó alkalmazása;
- felhasználói szintek szerinti jogosultságok elkülönítése;
- naplózás bekapcsolása és naplók megőrzésének biztosítása;
- jelszócsere kötelező érvényű beállítása (ha támogatott);
- tárolási idő és törlési ciklusok rögzítése és védelme;
- felesleges szolgáltatások kikapcsolása;
- távoli hozzáférés tiltása, ha a rendszer nem kapcsolódik hálózathoz.

Bár a területi térfigyelő kamera rendszer zárt, nem hálózati környezetben működik, az alábbiak kötelezőek:

- fizikai kábelezés sértetlenségének biztosítása;
- szabotázs elleni védelem alkalmazása;
- minden konfigurációs beavatkozás dokumentálása az üzemeltetési naplóban.

Az egységes konfigurációk a kamerákra, a rögzítőegységekre és az esetleges kezelőfelületekre egyaránt érvényesek.

További admin feladatok:

- minden új kamera és rögzítőt az egység beállításánál a konfigurációs baselinet alkalmazza
- minden módosítás megelőzően információbiztonsági hatásvizsgálatot végezzen
- minden konfigurációs módosítást dokumentáljon az üzemeltetési naplóban:
 - dátum,
 - elvégzett módosítás,
 - végrehajtó személy,
 - jóváhagyó,
 - hatásvizsgálat hivatkozása (ha szükséges).

9. A szabályzat tartalmának megismertetése

A szabályzat tartalmának megismerésének tényét az érintettek aláírásukkal kötelesek elismerni.

A szabályzat tartalmának megismertetéséről gondoskodni kell:

- amennyiben a szabályzatban, illetve mellékleteiben változás történt.

A szabályzatot a honlapon az adatvédelemmel kapcsolatos szekcióban közzé kel tenni.

10. Záró rendelkezések

A szabályzat mellékletét képezi:

- a kamera nyilvántartások telephelyenkénti bontásban,
- az adathordozó nyilvántartás,
- az incidens nyilvántartás,
- Éves Biztonsági Értékelési Terv és Eljárásrend

- Negyedéves ellenőrzési jegyzőkönyv

1. melléklet - Éves Biztonsági Értékelési Terv és Eljárásrend

Éves Biztonsági Értékelési Terv és Eljárásrend EIR01

Megfigyelő Területi térfigyelő kamera rendszerekre

1. Cél és hatály

Az éves biztonsági értékelési terv célja, hogy a szervezet megfigyelő területi térfigyelő kamera rendszereinek biztonságát, adatvédelmi megfelelőségét és a vonatkozó jogszabályoknak, valamint az ISO/IEC 27001 szabvány követelményeinek való megfelelést rendszeresen, dokumentált módon biztosítsa.

A terv kiterjed:

- a területi térfigyelő kamera rendszer fizikai és technikai elemeire,
- az adattárolásra és -hozzáférésre,
- a folyamatok és eljárások értékelésére,
- az adatvédelmi és jogszabályi megfelelőség ellenőrzésére.

2. Jogszabályi háttér

A „VVZrt térfigyelő kamera rendszer adatkezelési szabályzat v7 2025” dokumentum 1. mellékleteként szereplő „Éves Biztonsági Értékelési Terv és Eljárásrend” a területi térfigyelő kamera rendszer vonatkozásában részletesen rögzíti a biztonságértékelés célját, hatályát, az értékelésbe bevont környezetet (fizikai, informatikai és szervezeti környezet), az értékelésben részt vevő szerepköröket és felelőségeiket, az értékelés gyakoriságát, továbbá az alkalmazott értékelési módszertant és eljárásrendet.

A melléklet nevesíti a rendszerben megvalósított védelmi intézkedések értékelését, azok hatékonyságának vizsgálatát és továbbfejlesztési lehetőségeit, valamint előírja, hogy az éves ellenőrzés a 7/2024. (VI. 24.) MK rendeletben meghatározott, az adott biztonsági osztályhoz rendelt kötelező védelmi intézkedések teljesítésének vizsgálatára is kiterjed. A dokumentum meghatározza a jelentéskészítést, a kockázati besorolást, az intézkedési terv kialakításának és a vezetői jóváhagyásnak a folyamatát.

A biztonságértékelési terv és az éves értékelés megkezdését megelőzően a szervezet vezetője vagy az általa kijelölt felelős személy a mellékletben rögzített jóváhagyási blokk kitöltésével írásban hagyja jóvá az értékelés hatókörét, módszertanát, az értékelés ütemezését és az értékelésben részt vevő szerepköröket.

A fenti tartalom alapján az 1. mellékletben rögzített „Éves Biztonsági Értékelési Terv és Eljárásrend” a területi térfigyelő kamera rendszer vonatkozásában **teljesíti a 7/2024. (VI. 24.) MK rendelet 1. melléklet 5.2. pontjában, valamint az 1/2025. (I. 31.) SZTFH rendelet vonatkozó elemi követelményeiben meghatározott biztonságértékelési tervre vonatkozó elvárásokat**, ezért a szervezet külön, önálló biztonságértékelési terv dokumentum helyett az 1. melléklet alkalmazását tekinti az EIR szintű biztonságértékelési tervének.

A területi térfigyelő kamera rendszer ek működtetésére vonatkozóan az alábbi jogszabályok az irányadók:

- GDPR – (EU) 2016/679 rendelet,
- 2011. évi CXII. törvény az információs önrendelkezési jogról,
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi tevékenységekről,

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról,
- helyi adatvédelmi és biztonsági szabályzatok.

3. Éves értékelési ciklus

Az értékelés **évente egyszer**, a tárgyévet megelőző 12 hónap adatainak és működésének áttekintésével történik. Az éves ellenőrzés időpontját a szervezet információbiztonsági vezetője határozza meg. Az éves ellenőrzést az aktuális negyedéves ellenőrzéssel egyidőben kell elvégezni.

Extra értékelés csak akkor szükséges, ha:

- jelentős rendszertechnikai változás történik (pl. új kamera, új rögzítő, architektúraváltás),
- súlyos biztonsági incidens érinti a területi térfigyelő kamera rendszer t,
- hatóság vagy belső audit ezt előírja.

Az éves biztonsági értékelés az alábbi környezetben üzemelő területi térfigyelő kamera rendszer re terjed ki:

Fizikai környezet:

- A kamerák a szervezet ingatlanjainak belső és külső területein kerültek telepítésre, a vagyonvédelem támogatása céljából.
- A rögzítőeszközök biztonságos, hozzáférésben korlátozott helyiségekben található.

Informatikai környezet:

- A kamerák zárt hálózatba szervezve működnek.
- A rögzítők és kezelőeszközök elkülönített jogosultsággal érhetők el.
- A hálózati elérés tűzfalon és jogosultságkezelésen keresztül szabályozott.

Szervezeti környezet:

- A rendszer üzemeltetésében részt vevő szerepkörök: Gazdasági igazgató, rendszer-adminisztrátor, adatvédelmi tisztviselő.
- Az értékelés célja a meglévő védelmi intézkedések működésének, hatékonyságának és továbbfejlesztési lehetőségeinek vizsgálata.

A területi térfigyelő kamera rendszer EIR elemeire a szervezet által meghatározott biztonsági osztály szerinti, a 7/2024. (VI. 24.) MK rendeletben rögzített védelmi intézkedéseket kell alkalmazni. Az éves ellenőrzés kiterjed a vonatkozó kötelező kontrollok teljesítésének vizsgálatára.

4. Felelőségek

- **Gazdasági igazgató:** Petó Margit felel az értékelés lefolytatásáért.
- **Adatvédelmi tisztviselő (DPO):** Dr. Sümegi Zsombor felügyeli a GDPR-megfelelést.
- **IT rendszergazda:** Járvás Róbert biztosítja a technikai adatszolgáltatást.

5. Értékelési területek és módszertan

5.1. Területi térfigyelő kamera rendszer eszközeinek felülvizsgálata

- kamerák és rögzítők fizikai sértetlensége,
- látószög és rögzítési cél ellenőrzése,
- annak vizsgálata, hogy a rendszerelemekben történt változtatások megfelelnek-e a dokumentált biztonsági követelményeknek és megfelelően dokumentálásra kerültek-e,

- meghibásodások dokumentálása.

5.2. Hozzáférés-ellenőrzés

- felvételekhez való hozzáférési jogosultságok áttekintése,
- naplóbejegyzések és felhasználói hozzáférések felülvizsgálata,
- eltérések és jogosultsági anomáliák kezelése.
- A NIS2 előírásoknak megfelelően a területi térfigyelő kamera rendszer hozzáférési jogosultságait és naplóbejegyzéseit negyedévente felül kell vizsgálni. A negyedéves ellenőrzés eredménye dokumentálásra kerül, és az éves értékelés részeként is felhasználható.

5.3. Rögzített felvételek biztonsága

- adattárolási idők betartása,
- adattörlési és archiválási folyamatok ellenőrzése,
- a jogosultsági szintek, beállítások, naplók és verziók vizsgálata,
- titkosítás és jelszavak vizsgálata.
- A területi térfigyelő kamera rendszer rögzítési adataihoz kapcsolódó mentési és visszaállítási folyamatokat évente legalább egyszer tesztelni kell a NIS2 követelményeknek megfelelően. Az értékelés kiterjed a mentések meglétére, épségére, a visszaállítási teszt eredményeire.

5.4. Technikai megfelelés

- a rendszerelemek konfigurációja megfelel-e az egységes baseline-nak
- szoftverfrissítések és firmware-ek állapota,
- hálózati elszigetelés vizsgálata,
- naplófájlok rendszeressége és sértetlensége.
- A területi térfigyelő kamera rendszer t érintő konfigurációs, hardveres vagy szoftveres változásokat dokumentált változáskezelési folyamat szerint kell kezelni. Az éves értékelés során vizsgálni kell, hogy a változások megfelelnek-e a 7/2024. (VI. 24.) MK rendelet 5.19–5.28. pontjaiban meghatározott követelményeknek.
- Az éves értékelés kiterjed a kamerák és rögzítők hálózati kommunikációjának titkosítási állapotára, a TLS/HTTPS használatára, a hálózati elkülönítés megfelelésére és az alapértelmezett szolgáltatások tiltásának ellenőrzésére.

5.5. Adatvédelmi megfelelés

- kamerák elhelyezése megfelel a „szükségesség és arányosság” elvének,
- piktogramok és adatvédelmi tájékoztatók megléte,
- képfelvételt érintő DPIA felülvizsgálata.

5.6. Ellátási lánc kockázatok

A területi térfigyelő kamera rendszerhez kapcsolódó szállítói és beszállítói kockázatokat évente értékelni kell, különös tekintettel az EoL/EoS támogatottságra, firmware-ellátottságra és a gyártóval kapcsolatos biztonsági kockázatokra.

5.7. Dokumentációk

A területi térfigyelő kamera rendszerhez kapcsolódó dokumentumok (használati útmutatók, üzemeltetési dokumentációk stb.) rendelkezésre álló példányainak ellenőrzése, hatályosságuk ellenőrzése.

6. Dokumentálás

Minden értékelésről jegyzőkönyvet kell készíteni, amely tartalmazza:

- az ellenőrzés dátumát,
- az ellenőrzést végző személyek adatait,
- az értékelt területeket és megállapításokat,
- a feltárt kockázatokat és ajánlott intézkedéseket,
- a határidőket és felelősöket.

Amennyiben a konfiguráció eltér a baseline-tól:

- az eltérést azonnal dokumentálni kell;
- kockázatértékelést kell végezni;
- szükség esetén javító intézkedést kell elrendelni;
- az eltérést a következő éves értékelés során felül kell vizsgálni.

7. Kockázatelemzés és intézkedések

A megállapításokat kockázati besorolással kell ellátni. Az intézkedések:

- **Kötelező:** súlyos vagy magas kockázat esetén azonnali.
- **Javasolt:** közepes kockázat esetén.
- **Opcionális:** alacsony kockázat esetén.
- Az éves értékelés során vizsgálni kell, hogy a területi térfigyelő kamera rendszerre vonatkozó üzletmenet-folytonossági és helyreállítási követelmények teljesülnek-e, valamint hogy a rögzítő meghibásodása esetén biztosított-e a működés folytonossága.

8. Éves ütemezés

Az éves értékelés **egy alkalommal**, a szervezet által meghatározott időpontban kerül végrehajtásra. A korábbi havi bontás törölve, mivel az eljárás évente egyszeri felülvizsgálatra épül.

9. Eljárásrend

9.1. Előkészítés

- auditlista frissítése,
- érintett felelősök értesítése.

9.2. Helyszíni ellenőrzés

- kamerák és eszközök vizsgálata,
- rögzítési folyamatok elemzése.

9.3. Dokumentumellenőrzés

- belső szabályzatok,
- adatvédelmi tájékoztatók,
- hozzáférési listák.

9.4. Jelentés összeállítása

- megállapítások,

- kockázati besorolás,
- intézkedési terv.

A biztonságértékelés eredményeit és az intézkedési tervet a Gazdasági igazgató, az információbiztonsági felelős, az adatvédelmi tisztviselő és az érintett szervezeti egység(ek) vezetői számára hozzáférhetővé kell tenni, és a megállapítások megismertetéséről dokumentált módon gondoskodni kell.

9.5. Jóváhagyás és nyomonkövetés

- vezetőség jóváhagyása,
- intézkedési feladatok kiosztása,
- utóellenőrzés.

9.6. Vezetői jóváhagyás

A biztonságértékelési tervet és az éves biztonságértékelés megkezdését megelőzően a szervezet vezetője vagy az általa kijelölt meghatalmazott felelős jóváhagyja. A jóváhagyás kiterjed:

- az értékelés hatókörére,
- az alkalmazott értékelési módszertanokra,
- az értékelő személy(ek) kijelölésére,
- valamint az értékelés ütemezésére.

A jóváhagyás írásban történik, és a dokumentumhoz csatolt aláírási blokk tartalmazza a jóváhagyó nevét, pozícióját, dátumot és aláírását.

Jóváhagyási blokk:

Név: Hotgosi Zsolt

Pozíció: vezérigazgató

Dátum:

Aláírás:

9.7. Incidenskezelési követelmények

A területi térfigyelő kamera rendszert érintő, NIS2 szerinti jelentős információbiztonsági incidens esetén a szervezet az 1/2025. SZTFH rendelet és a 418/2024. Korm. rendelet szerinti bejelentési kötelezettséget teljesíti (24 órás előzetes, 72 órás részletes jelentés). Az éves értékelés során az incidenskezelési folyamat és a bejelentések megfelelőségét is vizsgálni kell.

10. Mellékletek

10.1. Kamera Ellenőrzési Jegyzőkönyv Sablon

Ellenőrzés dátuma:

Ellenőrzést végző személy(ek):

Helyszín / telephely:

Értékelt terület(ek):

- Kamerák fizikai állapota
- Rögzítők és tárolók állapota

- Felvétel-minőség és működőképesség
- Jogosultságkezelés és hozzáférések
- Adattárolási idők betartása
- Naplózás és eseménykezelés
- GDPR és Infotv. Megfelelőség
- Dokumentációk

Megállapítások:

.....

Feltárt kockázatok:

.....

Kockázati besorolás: (alacsony / közepes / magas)

Javasolt intézkedések:

Felelős:

Határidő:

Jóváhagyó:

10.2. Kockázatmátrix

Kockázat szintje	Leírás
Alacsony	Olyan eltérés, amely nem veszélyezteti a Kamera működését vagy az adatvédelmet. Javítása ajánlott.
Közepes	A működést vagy a jogszabályi megfelelést részben befolyásoló hiba. Javítása szükséges.
Magas	Azonnali intézkedést igénylő, jogsértést vagy biztonsági kockázatot jelentő probléma.

Valószínűség skála:

- **1 – Ritka:** szinte soha nem fordul elő
- **2 – Lehetséges:** évente előfordulhat
- **3 – Gyakori:** rendszeresen előfordul

Hatás skála:

- **1 – Alacsony:** nincs működési vagy jogi következmény
- **2 – Közepes:** kisebb működési fennakadás vagy átmeneti nemmegfelelés
- **3 – Súlyos:** jogsértés, adatvédelmi incidens, szolgáltatás-kiesés

Kockázati szint képlet:

Valószínűség × Hatás = Kockázat (1–9)

Kockázati érték Szint

1–3 Alacsony

4–6 Közepes

7–9 Magas

10.3. Hozzáférés-nyilvántartási sablon**Felhasználó neve:****Pozíció:****Hozzáférési szint:** (megtekintés / export / törlés / adminisztrátor)**Hozzáférés engedélyezésének dátuma:****Engedélyező neve:****Megjegyzés:**

- Kamera eszközlétár sablon
- Éves auditlista
- Kockázatértékelési mátrix
- Hozzáférés-nyilvántartási sablon

10.4 A biztonságértékelési jelentés terjesztése

A biztonságértékelés eredményét összefoglaló jelentést a szervezet az alábbi szerepkörök számára teszi elérhetővé, a szerepkörökhöz tartozó jogosultságoknak megfelelően:

- **Szervezet vezetése:** Horgosi Zsolt, Pető Margit stratégiai döntéshozatal és erőforrás-hozzárendelés céljából.
- **Információbiztonsági felelős:** Schiroky Vilmos az intézkedési terv végrehajtásának felügyeletéhez.
- **Adatvédelmi tisztviselő (DPO):** Dr. Sümegi Zsombor a GDPR-megfelelőség ellenőrzése miatt.
- **Rendszergazda:** Járvás Róbert a megállapítások műszaki végrehajtása érdekében.

A jelentéshez való hozzáférés dokumentált módon történik, a meghatározott megőrzési időn keresztül. A terjesztés nyilvántartása tartalmazza a megismerők listáját, dátumát és a szerepköröket.

2. melléklet - Kamerák negyedéves ellenőrzés jkv

#	Ellenőrzési pont	Részletezés	Megfelel	Nem felel meg	N/A	Megjegyzés
1	Fizikai állapot	Kamera és rögzítő eszközök sértetlensége, kábelezés, rögzítettség	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2	Szabotázsjelek	Elmozdítás, letakarás, rongálás jelei	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	Tápellátás	Folyamatos áramellátás, szünetmentes tápegység állapota	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4	Környezeti hatás	Kültéri kamerák időjárás-állósága, tok állapota, kondenzáció	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

5	Szoftver-/firmware-verzió	Legfrissebb gyártói verziók telepítve? Frissítés elérhető?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6	Jogosultságok felülvizsgálata	Felhasználói hozzáférések listája, admin és operátor szerepkörök jogosultságai	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7	Inaktív/hibás fiókok törlése	Nem használt fiókok eltávolítva, hozzáférés-visszavonás nyilvántartva	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
8	Naplóbejegyzések megléte	Eseménynaplók, be-/kilépések, konfigurációváltozások naplózva?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9	Napló telítettsége	Naplóállomány mérete, forgatás, archiválás működik-e	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
10	Felvétel visszakeresése	Felvételek visszakereshetősége, szegmentálás, napok száma	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
11	Tárhely telítettség	Felvételtároló (NVR, NAS stb.) szabad kapacitása, automatikus felülírás	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
12	Megőrzési idő ellenőrzése	Megfelel a szabályzatban előírt napos határidőnek?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
13	IP-konfiguráció	IP-címek, port forwarding, VPN-ek, NAT beállítások ellenőrzése	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
14	Külső kapcsolatok	Mobilapp, felhőkapcsolat, távoli hozzáférés konfigurációja	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
15	Teszt-rögzítés	Minden kamera rögzít-e, próbafelvétel készítése tesztcélből	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
16	Mozgásérzékelő/riasztás	Mozgásra indított rögzítés és riasztás beállítások ellenőrzése	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
17	Értesítések működése	Értesítések (kamera kiesés, telítettség, leállás) tesztelése	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
18	Változások dokumentálása	Változások (jogosultság, IP, firmware, beállítás) naplózva?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
19	Ellenőrzési dokumentáció	Az ellenőrzésről készült jegyzőkönyv/sablon kitöltve	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

3. melléklet Területi térfigyelő kamera rendszer felvételeinek lekérése és hozzáférése

Cél

Ez az eljárás biztosítja a területi térfigyelő kamera rendszer felvételeinek biztonságos, jogszerű és hatékony lekérését a Szervezeti incidensek vagy jogszerű megkeresések esetén. Meghatározza az érvényesítés, jóváhagyás és átadás lépéseit, miközben biztosítja az adatvédelmi előírásoknak való megfelelést.

Hatály

Ez a szabványos működési eljárás (SOP) minden olyan személyre vonatkozik, aki részt vesz a területi térfigyelő kamera rendszer felvételeinek lekérésében, beleértve:

Biztonsági személyzet (IT rendszergazda)

Adatvédelmi tisztviselők

Vezetőség (Gazdasági igazgató)

Eljárás

- Kérelem kezdeményezése

A területi térfigyelő kamera rendszer felvételeinek megtekintésére vagy lekérésére irányuló kérelmet az alábbi okokból lehet benyújtani:

Szervezeti incidens (pl. biztonsági esemény, munkahelyi vizsgálat).

Jogszerű megkeresés (pl. bírósági idézés, hatósági megkeresés).

- Kérelem érvényesítése

A kérelmezőnek hivatalos kérelmet kell benyújtania, amely tartalmazza:

A hozzáférés célját (az incidens részleteit vagy a jogi indoklást).

A szükséges felvétel konkrét dátumát és időpontját.

A kérelmet a kijelölt felelős személy (Gazdasági igazgató) felülvizsgálja és ellenőrzi annak érvényességét.

- Tisztázás (ha szükséges)

Ha a kérelem nem egyértelmű (pl. hiányos időpont vagy indoklás), a kérelmezőt fel kell keresni további részletekért.

- Jóváhagyási folyamat

A kérelmet továbbítani kell a Vezetőség részére (elsődlegesen adatvédelmi tisztviselő) jóváhagyás céljából.

A Vezetőség a kérelmet az alábbi szempontok alapján értékeli:

A Szervezeti szabályzatokkal való összhang.

Jogi és szabályozási követelményeknek való megfelelés (pl. GDPR, helyi adatvédelmi törvények).

Jóváhagyási döntés:

Jóváhagyva: A folyamat folytatódik a felvétel lekérésével.

Elutasítva: A kérelmező írásbeli indoklást kap, és az eljárás lezárul.

- Felvétel lekérése és kezelése

Hozzáférés: Csak kijelölt, jogosult személy (IT rendszergazda) férhet hozzá és töltheti le a felvételt.

Letöltés: A felvételt biztonságos módon kell letölteni és védett környezetben tárolni.

Védelem: A letöltött felvételt titkosítani vagy jelszóval védeni kell az illetéktelen hozzáférés megakadályozása érdekében.

- Átadás a kérelmezőnek

A védett felvétel átadásra kerül az eredeti kérelmezőnek vagy az arra jogosult félnek.

Az átadásról nyilvántartást kell vezetni az auditálás biztosítása érdekében.

- Folyamat lezárása

Az eljárás lezártnak tekinthető, ha a felvétel átadásra került, vagy ha a kérelmet elutasították és az indoklás dokumentálva van.

Szerepkörök és felelőségek

Szerepkör	Felelőség
Kérelmező	Hivatalos kérelmet nyújt be, amely tartalmazza az indoklást, valamint a felvétel pontos dátumát és időpontját.
Vezetőség (Gazdasági igazgató)	Érvényesíti a kérelmet, és szükség esetén pontosítja a részleteket.
Vezetőség (Adatvédelmi tisztviselő)	Jóváhagyja vagy elutasítja a kérelmet a jogszabályi és Szervezeti megfelelés alapján.
IT rendszergazda	Lekéri, letölti és biztonságosan tárolja a felvételt.
Kérelmező / Jogosult fél	Átv teszi a felvételt és igazolja az átvételt.

Megfelelőség és nyilvántartás

Minden kérelmet, jóváhagyást és átadást dokumentálni kell, és biztonságosan kell tárolni az auditálhatóság érdekében.

A felvételekhez való hozzáférésnek meg kell felelnie a Szervezet Adatvédelmi Szabályzatának és a vonatkozó jogszabályoknak.

Fogalom meghatározások

Területi térfigyelő kamera rendszer -felvétel: A Szervezet megfigyelőrendszere által rögzített videófelvétel.

Kijelölt személy: Felelős a felvételek átadásért és megőrzésért.

Vezetőség: Elbírálja és jóváhagyja a kérelmeket.

