

Raport de analiza de risc la securitatea fizica Nr. 115 Rev. 01

Am luat la cunostinta analiza de risc.

Reprezentant beneficiar: _____

Raportul de evaluare si propuneri de tratare a riscului la securitatea fizica pentru obiectivul

GRADINITA CU PROGRAM PRELUNGIT NR. 13 BISTRITA

Societate prestatoare: SC ARIOLA PRODCOM SRL**Nr. Inreg. Doc.: 115 / 11.05.2021****Evaluator risc securitate fizica:****TOTH MÁRTON****Nr. Inreg. RNERSF: 413/22.12.2014****Reprezentant legal:****TOTH MÁRTON****Asumat beneficiar****Nr. /****Reprezentant:****POP MARIANA STEFANIA LIANA - Director**

CUPRINS

Cap. 1. Nominalizarea unitatii, obiectul de activitate si tipul evaluarii

1.1 Denumirea si datele de identificare ale obiectivului evaluat

1.2 Scop

1.3 Reglementari si normative

1.4 Termeni si definitii

1.5 Date generale referitoare la obiectiv

Cap. 2. Amplasarea geografica a unitatii, vecinatati, cai de acces, alti factori externi cu impact asupra activitatii unitatii

Cap. 3. Cadrul organizational intern, politici si responsabilitati privind securitatea fizica

3.1 Descrierea obiectivului

3.2 Documente aferente sistemului de securitate

3.3 Aspecte functionale

3.4 Masuri de securitate existente in obiectiv

3.5 Subcontractori pentru servicii de securitate

Cap. 4. Sursele de risc la securitatea fizica, zonele de impact, evenimentele si cauzele riscului identificate pentru unitatea evaluata, precum si potentialele consecinte asupra persoanelor si activitatii

4.1 Stabilirea contextului

4.2 Incadrarea unitatii

4.3 Stabilirea activelor relevante

4.4 Analiza de impact

4.5 Zonarea obiectivului

4.6 Sursele de amenintare

4.7 Determinarea si evaluarea amenintarilor la adresa activelor relevante**4.8 Enuntarea riscurilor la securitatea fizica****Cap. 5. Analizarea riscurilor identificate****5.1 Scenariile de amenintare****5.2 Determinarea indicilor de risc****Cap. 6. Estimarea riscurilor la securitate fizica**

Cap. 7. Stabilirea cerintelor, masurilor si mecanismelor de securitate pentru sistemul ce urmeaza a fi implementat, de ordin structural, tehnic, tehnologic si operational

Cap. 8. Estimarea costurilor de securitate in functie de masurile de securitate propuse si nivelul de risc asumat

Cap. 9. Concluzii

Cap. 1. Nominalizarea unitatii, obiectul de activitate si tipul evaluarii

1.1 Denumirea si datele de identificare ale obiectivului evaluat

Prezentul raport de analiza de risc la securitatea fizica este efectuat pentru obiectivul

GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA

Datele de identificare a obiectivului:

- Adresa: Aleea Basmului, Nr. 2, Bistrita, jud. Bistrita-Nasaud.
- Telefon: 0263 211 259.
- Email: gradinita_nr13@yahoo.com.
- Reprezentant: POP MARIANA STEFANIA LIANA – Director.
- CIF: 29871150
- Obiectul de activitate: **COD CAEN – 8510 – Invatamant prescolar.**

GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA se incadreaza in categoria : **Unitati de interes public.**

1.2 Scop

Analiza riscurilor la securitatea fizica constituie documentul de fundamentare a masurilor de securitate adoptate de companie / unitate si, implicit, a planului de paza, a proiectului sistemului de securitate si a procedurilor de securitate aferente unitatii respective, in conformitate cu prevederile Legii nr. 333/2003, a HG nr. 301/2012 si a HG nr. 1002/2015.

In conformitate cu HG nr. 301/2012, HG nr.1002/2015 si Instructiunile MI nr. 9/2013, analiza riscurilor se aplica fiecarei unitati si se are in vedere fiecare categorie de active relevante pentru unitatea respectiva.

Elaborarea analizei riscurilor are in vedere aspectele de conformitate cu reglementarile mentionate mai sus si cu alte reglementari care trateaza aspecte de securitate fizica, inclusiv sub aspectul respectarii tuturor prescriptiilor aplicabile unitatii.

TIPUL EVALUARII: REVIZUIRE

Conform Instructiunii nr. 9/01.02.2013 al MAI – cap. II, art. 4, al. 4, lit. c. .

PERIOADA DE EVALUARE: 11.05.2021 – 14.05.2021.

1.3 Reglementari si normative

Prezenta metodologie este aliniata cu urmatoarele reglementari si normative:

- Legea nr. 333/2003 - privind paza obiectivelor, bunurilor, valorilor și protectia persoanelor si modificarile aduse prin Legea nr.9/2007, Legea 40/2010;
- H.G. nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor si protectia persoanelor;
- H.G. nr. 1002/2015 pentru modificarea si completarea HG 301/2012 pentru aprobare Normelor metodologice de aplicare a Legii nr.333/2003 privind paza obiectivelor, bunurilor, valorilor si protectia persoanelor;
- SR ISO/IEC 31000 Managementul riscului; SR ISO/IEC 31010 Tehnici de analiza a riscului;
- Seria de standarde Sisteme de management al calității (SR EN ISO 9001:2008);
- Seria de standarde SR EN 50131 - Sisteme de alarmă. Sisteme de alarmă împotriva efracției și jafului armat;
- Seria de standarde SR EN 62676 - Sisteme de supraveghere video utilizate în aplicatii de securitate;
- Seria de standarde SR EN 60839 - Sisteme de alarma si de securitate electronica. Sisteme electronice de control al accesului.
- Seria de standarde SR EN 50518 - Centru de monitorizare și recepție a alarmelor;
- Standarde europene sau naționale de certificare a mijloacelor de protecție mecanofizică:
 - pentru unități de depozitare de securitate SR EN 1143-1:1997/A2,
 - pentru vitraje SR EN 356:2003, SR EN ISO 12543-2:2012,
 - pentru tâmplărie SR ENV 1627, SR ENV 1630).

1.4 Termeni si definitii

securitate fizica

starea de fapt in care riscul determinat de factorii de amenintare si vulnerabilitatile care pot pune in pericol viata, integritatea corporala sau libertatea persoanei ori pot aduce prejudicii valorilor detinute de unitati, se situeaza la un nivel acceptabil;

amenintare

factor intern sau extern ce are capacitatea de a exploata vulnerabilitatea unei unitati prin acte sau fapte ce creeaza dezechilibre ori instabilitati si genereaza stari de pericol asupra vietii, integritatii corporale sau libertatii persoanelor ori valorilor detinute;

vulnerabilitate

caracteristica de ordin fizic-arhitectural si operational a unei entitati, prin care aceasta este expusa distrugerii, agresiunii ori disfunctionalitatii in fata unei amenintari.

analiza de risc la securitatea fizica

activitate desfasurata pentru a identifica amenintarile si vulnerabilitatile care pot pune in pericol viata, integritatea corporala sau libertatea persoanei ori care pot aduce prejudicii valorilor detinute de unitati, in scopul determinarii impactului si evaluarii riscurilor de securitate si in baza careia se stabilesc masurile necesare pentru limitarea sau eliminarea acestora;

incident de securitate

eveniment produs, avand o evolutie necontrolata, care genereaza consecinte nedorite asupra persoanelor si/sau valorilor si/sau activitatilor in cadrul unei unitati si care necesita o actiune imediata pentru restabilirea situatiei anterioare;

masura de securitate

componenta de baza a unei solutii de securitate, corespunzatoare uneia sau mai multor amenintari si vulnerabilitati identificate conform analizei de risc si care are ca scop reducerea riscurilor asociate;

mecanisme de securitate

solutii care cuprind mai multe masuri de securitate, care functioneaza conform unor scenarii predefinite, pentru securizarea unuia sau mai multor obiective, atunci cand sunt amplasate in acelasi perimetru;

sistem de securitate

ansamblu integrat de masuri organizatorice, tehnice si procedurale care are scop obtinerea securitatii fizice pentru o organizatie sau obiectiv;

parametri interni si externi care genereaza si/sau modifica riscurile la securitatea fizica a unitatii

reprezinta contextul care poate cuprinde, dar nu se limiteaza la:

- 1 mediul cultural, social, politic, de reglementare, financiar, tehnologic, economic, natural si concurential, la nivel international, national, regional sau local;
- 2 factorii cheie si tendintele cu impact asupra obiectivelor organizatiei;
- 3 relatiile cu partile interesate, perceptiile si valorile acestora.

risc

efectul incertitudinii asupra realizarii obiectivelor

managementul riscului

activitati coordonate pentru a directiona si a controla o organizatie in ceea ce priveste riscul

politica referitoare la managementul riscului

declaratia cu privire la intentiile si orientarile generale ale unei organizatii referitoare la managementul riscului

proces de management al riscului

aplicarea sistematica a politicilor, procedurilor si practicilor de management la activitatile de comunicare, de consultare, de stabilire a contextului, precum si la identificarea, analiza, evaluarea, tratarea, monitorizarea si revizuirea riscului

parte interesata

persoana sau organizatie care poate afecta, poate sa fie afectata, sau se poate simti afectata de o decizie sau de o activitate

perceptia riscului

punctul de vedere al partii interesate asupra unui risc

stabilirea contextului

definirea parametrilor interni si externi care urmeaza sa fie luati in considerare in managementul riscurilor, precum si determinarea domeniului de aplicare si a criteriilor de risc pentru politica referitoare la managementul riscului

criterii de risc

termenii de referinta fata de care este evaluata semnificatia unui risc

evaluarea riscului

proces global care cuprinde identificarea riscului, analiza riscului si estimarea riscului

identificarea riscului

proces de descoperire, recunoastere si descriere a riscurilor

descriere a riscului

prezentare structurata a riscului ce contine de obicei patru elemente: surse, evenimente, cauze si consecinte

sursa riscului

element care, singur sau in combinatie cu altele, are potentialul intrinsec de a produce un risc

eveniment

aparitie sau modificare a unui anumit set de imprejurari

proprietarul riscului

persoana sau entitate cu responsabilitatea si autoritatea de a gestiona un risc

analiza riscului

procesul de intelegere a naturii riscului si de determinare a nivelului de risc

plauzibilitate

posibilitatea ca ceva sa se intample

consecinta

efectul unui eveniment care afecteaza obiectivele

vulnerabilitate

caracteristica de ordin fizic - arhitectural si operational a unei entitati, prin care aceasta este supusa distrugerii, agresiunii ori disfunctionalitatii in fata unei amenintari

matrice de risc

instrument pentru clasificarea si afisarea riscurilor, prin definirea categoriilor de consecinte si de plauzibilitati

nivel de risc

marimea unui risc sau a unei combinatii de riscuri, exprimata in termeni de combinatie a consecintelor si a plauzibilitatii acestora

estimarea riscului

procesul de comparare a rezultatelor analizei riscului cu criteriile de risc pentru a determina daca riscul si / sau marimea acestuia sunt acceptabile sau tolerabile

acceptarea riscului

decizie in cunostinta de cauza de asumare a unui anumit risc

tratarea riscului

proces de modificare a riscului

NOTA 1 - Tratarea riscului poate include:

- *evitarea riscului prin luarea deciziei de a nu incepe sau de a nu continua activitatea care genereaza riscul;*
- *asumarea sau cresterea riscului pentru a urmari o oportunitate;*
- *indepartarea sursei de risc;*
- *modificarea plauzibilitatii;*
- *modificarea consecintelor;*
- *partajarea riscului cu o alta parte sau parti (inclusiv contracte si finantare a riscului); si*
- *mentinerea riscului printr-o decizie argumentata.*

mijloc de control

masura care modifica riscul

NOTA 2 - Mijlocul de control include orice proces, politica, dispozitiv, practica sau alte actiuni care modifica riscul.

evitarea riscului

decizie argumentata de a nu fi implicat in, sau de a se retrage dintr-o activitate pentru a nu fi expus la un anumit risc

partajarea riscului

forma de tratare a riscului care implica distribuirea consimtita a riscului cu alte parti

finantarea riscului

forma de tratare a riscului care implica acorduri pentru situatii neprevazute referitoare la furnizarea de fonduri pentru a face fata sau a modifica eventualele consecinte financiare

retinerea riscului

acceptarea castigurilor sau pierderilor potentiale rezultate dintr-un anumit risc

risc rezidual

riscul ramas dupa tratarea riscului

rezilienta

capacitatea de adaptare a unei organizatii intr-un mediu complex si in schimbare

activ

reprezinta tot ceea ce este relevant pentru companie / obiectiv din punctul de vedere al reglementarilor de securitate

1.5 Date generale referitoare la obiectiv

Evaluarea riscurilor la securitatea fizica la GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA are ca scop incadrarea in prevederile HG nr. 301/2012 si HG nr.1002/2015. Se urmareste, de asemenea, identificarea si evaluarea amenintarilor si vulnerabilitatilor care pot conduce la riscuri inacceptabile, precum si masurile de securitate care pot determina reducerea acestor riscuri in contextul organizatoric, strategic si bugetar al GRADINITEI CU PROGRAM PRELUNGIT NR. 13 - BISTRITA.

GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA este o unitate de interes public cu specific de invatamant prescolar, infiintata conform Deciziei nr. 355 din 16.12.1974 a Comitetului Executiv al Consiliului popular al judetului Bistrita-Nasaud (ANEXA NR. 4) si a Hotararii Nr. 905/2002 al Consiliului Local al Municipiului Bistrita privind actualizarea inventarului bunurilor care apartin domeniului public al Municipiului Bistrita (ANEXA NR. 5).

GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA se incadreaza in categoria:

Unitati de interes public,

avand ca obiect de activitate **Invatamant prescolar – cod CAEN 8510.**

Cap. 2. Amplasarea geografica a unitatii, vecinatati, cai de acces, alti factori externi cu impact asupra activitatii unitatii

Obiectivul GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA este amplasat in Bistrita, jud. Bistrita-Nasaud, STR. BASMULUI, NR. 2.



Vedere de sus



Vedere de sus



Vedere de sus

Descrierea vecinatatilor obiectivului:

NORD: Punct de transformare (Electrica), parcuri auto rezidentiale, blocuri de locuinte.



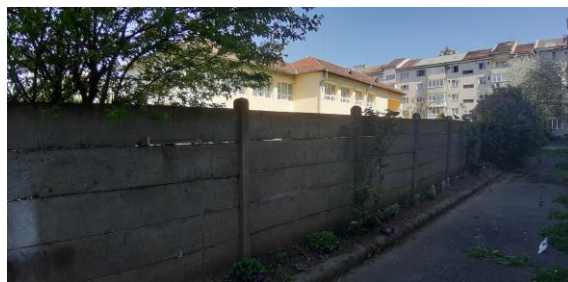
Cluj-Napoca, str. Macesului nr. 58F,

PUNCT DE LUCRU: Cluj-Napoca, str. Intre Lacuri, nr. 45, tel. 0264-432616

e-mail: alarm@ariola.ro; URL: www.ariola.ro

DOCUMENT CONFIDENTIAL

SUD: blocuri si case de locuit.



EST: blocuri de locuinte.



VEST: case de locuit si curti.





Disimulare/fuga greoaie – 35 m

Caracteristicile vecinatatilor obiectivului:

- Criminalitate caracteristica zonala: unitate situata in judet cu rata a criminalitatii scazuta (ANEXA NR. 6).
- Criminalitate caracteristica locala: municipiu cu o rata a criminalitatii ridicata (ANEXA NR. 7).
- Accesibilitate: posibilitate de disimulare/fuga greoaie.
- Vecinatati: rezidente.
- Caracteristici locale exterioare: zona cu trafic pietonal si/sau rutier mediu.

Cap. 3. Cadrul organizational intern, politici si responsabilitati privind securitatea fizica

3.1 Descrierea obiectivului

Obiectivul este compus din 2 corpuri de cladire.

CORP 1: Gradinita - constructie din anii 1970, cu regim de inaltime S+P+E+Pod, realizat din caramida pe cadre din beton cu suprafata construita de 797 mp si suprafata desfasurata de 1506 mp.

In urma lucrarilor de modernizare ce vor avea loc in cursul anului 2021 se vor obtine compartimentarile din plansele din ANEXA NR. 8.



CORP 2: Centrala termica si magazie – situata in partea de vest a curtii interioare, constructie pe un singur nivel, realizat din caramida pe cadre din beton cu suprafata de 28 mp.



CURTE INTERIOARA: cu o suprafata de 3820 mp conform extras CF Nr. 51141/21.10.2020 (ANEXA NR. 14), imprejmuita cu un gard din placi de beton cu stalpi din beton, cu inaltimea de 2,20 m.



Caracteristicile structurii obiectivului:

- Protectie suprafete vitrate: suprafete vitrate necertificate.
- Tâmplarie: usi si ferestre din elemente constructive necertificate.
- Acces clienti: usa simpla.
- Pereti exteriori si zone de fixare tâmplarie: beton si zidarie groasa (min. 150 mm).
- Compartiment operator: incinta distincta din elemente constructive necertificate.
- Dotare ghiseu de lucru cu clientii: ghiseu fara dulap de casierie cu temporizare sau casa de marcat cu sertar de depozitare.
- Amplasare si dotare: seif certificat antifoc ancorat, amplasat in spatiu anume destinat si amenajat.
- Protectie bunuri expuse: unitatea nu expune bunuri pentru comercializare/vizionare.
- Trasee de manipulare interioara numerar: prin zone accesibile clientilor.
- Puncte de transfer catre exterior: usa de acces accesibila clientilor.
- Amplasare procesare: incinta distincta din elemente constructive necertificate.
- Amplasare echipamente: incinta distincta din elemente constructive necertificate.

Schita obiectivului este prezentata in ANEXA NR. 8.

Tipul de proprietate asupra obiectivului: Proprietate publica a Municipiului Bistrita.

Principalele activitati desfasurate in obiectiv sunt:

- activitati educationale (invatamant prescolar)
- pregatirea si servirea mesei
- pastrare documente in legatura cu operatiuni curente si/sau de sprijin pentru activitatile curente si accidentale;
- operatiuni cu sistemul tehnic de securitate;
- mentenanta sistemelor tehnice (alimentare cu energie electrica, comunicatii, tehnologia informatiei, securitate, echipamente specifice activitatii, etc.);
- activitati administrative.

3.2 Documente aferente sistemului de securitate

Nu au fost identificate documente referitoare la sistemul tehnic de securitate.

3.3 Aspecte functionale

ORAR: LUNI-VINERI: 6:00 – 18:00.

Numar angajati: 21, in doua schimburi. Organigrama prezentata in ANEXA NR.9.

Numar de copii inscriși in grupele gradinitei: 152.

Conform informatiilor furnizate de reprezentantul unitatii nivelul de operatiuni cu numerar/zi nu depaseste suma de 10.000 lei. Unitatea nu depoziteaza numerar pe timpul noptii, sumele incasate reprezentand taxele de hrana fiind transportate si depuse in aceeasi zi la banca de catre persoane desemnate pentru acest scop (administratorul gradinitei).

Principalele caracteristici functionale ale obiectivului sunt:

- Depozitare numerar (noaptea): mic < 10000 eur.
- Nivel operatiuni cash: mic < 10000 eur / zi.
- Numar salariati: >3.
- Existenta procedurilor de lucru de securitate: proceduri existente.
- Intreruperi alimentare energie electrica: ups echipamente securitate si comunicatii.
- Intreruperi comunicatii: rare.

3.4 Masuri de securitate existente in obiectiv

Descrierea generala a masurilor de securitate din obiectiv:

Sistemul de detectie a patrunderii prin efracție acopera partial obiectivul, in zonele sensibile (holuri de acces, birou director, administrator, zona de preparat hrana).

Centrala sistemului de alarmare la efracție (tip PARADOX) este montata pe peretele din vecinatatea usii de acces din latura sudica.



Tastatura sistemului de alarmare la efracție este montata pe peretele din vecinatatea usii de acces din latura sudica.



Usa de acces de pe latura sudica este asigurata cu un sistem de interfonie cu dispozitiv electromecanic de blocare a usii cu control din interior.



Sistemul de alarmare la efracție este completat cu 2 butoane de panică mobile (telecomenzi) pentru semnalizarea stării de pericol din biroul administrativ și biroul directorului.



Valorile monetare sunt pastrate pe timpul zilei intr-un dulap de documente certificat antiincendiu, amplasat in biroul administratorului, prevazut cu detector de soc.



Dulapul de depozitare documente folosit pentru depozitarea valorilor banesti **nu este certificat** antiefracție conform SR EN 1143-1:1997/A2,

Sistemul de supraveghere video este compus din inregistrator video 4 canale si 4 camere video ce asigura preluarea imaginilor din zonele: intrare EST, casa scarii, curte VEST, curte SUD.

Inregistratorul video este montat in biroul directorului, intr-un dulap de echipamente IT, prevazut cu incuietoare mecanica si asigura preluarea de imagini pentru 33 de zile.



Sistemul este prevazut cu un UPS de tip APC 700.



Principalele caracteristici ale masurilor de securitate existente in obiectiv:**Obiectivul beneficiaza de:**

- Detectia patrunderii prin efracție
- Semnalizare stare de pericol personal
- Supraveghere video
- Stocare imagini video pentru 20 zile
- Acces controlat zona acces
- Interventie prin personal specializat
- Conectare la dispecerizat de monitorizare
- Semnalizare fortare seif

Obiectivul nu beneficiaza de:

- Calitate imagini care permite recunoasterea persoanelor
- Paza umana

Transport valori: neorganizat.

3.5 Subcontractori pentru servicii de securitate

Serviciile de paza, monitorizare, interventie, instalare si mentenanta a sistemelor de securitate sunt:

- Mentenanta sistemului tehnic de securitate este asigurata de catre SC AMG GROUP PROTECT SRL in baza contractului nr. 187 din 10.03.2021 (ANEXA NR. 10).
- Transportul numerarului NEORGANIZAT;
- Monitorizarea obiectivului este asigurata de catre SC ROMANIAN SECURITY SYSTEMS SRL in baza contractului Nr. RSBN 3704 din 31.08.2018 (ANEXA NR. 11).

Cap. 4. Sursele de risc la securitatea fizica, zonele de impact, evenimentele si cauzele riscului identificate pentru unitatea evaluata, precum si potentialele consecinte asupra persoanelor si activitatii

4.1 Stabilirea contextului

Pentru stabilirea contextului:

1. Au fost purtate discutii cu reprezentantul obiectivului GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA : POP MARIANA STEFANIA LIANA-Director.
2. A fost elaborat un chestionar de culegere a datelor care a fost transmis responsabililor de unitati (ANEXA NR. 12).
3. Au fost efectuate verificari si au fost culese date din unitate, informatiile fiind completate impreuna cu reprezentantii beneficiarului in formularul chestionar.
4. Au fost consultate urmatoarele documentele:
 - Decizii si hotarari ale consiliului local
 - Certificat de atestare fiscala (ANEXA NR. 13)
 - Certificat de inregistrare fiscala (ANEXA NR. 14)
 - Coeficienti de criminalitate
 - Organigrama
 - Schite si planuri
 - Contracte servicii de mentenanta si monitorizare sisteme de securitate
 - Procedura operationala privind asigurarea securitatii si sigurantei elevilor in perimetrul unitatilor scolare
 - Procedura operatională privind protecția muncii în salile de grupa si spatiile auxiliare
 - Procedura operatională psi și gestionarea situațiilor de criză
 - Procedura operatională privind securitatea ocupationala, protectia muncii, prevenirea si stingerea incendiilor.

A fost analizat istoricul incidentelor pe ultimele doua semestre. In evidentele obiectivului: Nu au fost inregistrate incidente privind securitatea fizica a obiectivului in ultimii 3 ani.

In zona de dispunere a obiectivului, in vecinatatea de zonei de acces in curtea obiectivului se identifica un punct de transformare zonal al Companiei Electrice, iar in curtea obiectivului s-a identificat un autoturism apartinand personalului gradinitei, aspecte pe care le consideram a avea un caracter deosebit.

4.2 Incadrarea unitatii

Obiectivul GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA se incadreaza, din punctul de vedere al reglementarilor in vigoare, in categoria:

UNITATI DE INTERES PUBLIC

4.3 Stabilirea activelor relevante

In urma aplicarii prevederilor metodologiei de analiza a riscurilor la securitatea fizica au fost identificate 50 active; urmatoarele active sunt considerate relevante:

1. administrator
2. alimentare cu apa
3. alimentare cu energie electrica
4. alimentare cu gaze naturale
5. autoturisme
6. alte echipamente
7. alte instalatii specifice activitatii
8. alimente si materie prima pentru prepararea alimentelor
9. alte echipamente specifice activitatii
10. angajati
11. bunuri ale copiilor, apartinatorilor
12. bunuri ale personalului propriu si contractual
13. centrala termica
14. colectare numerar
15. deseuri
16. deseuri medicale
17. director / personal de conducere

-
18. documente din arhiva curenta
 19. documente legate de securitate
 20. documente operationale
 21. documente protejate (continand date cu caracter personal)
 22. dulapuri de documente
 23. echipament de comunicatii
 24. echipamente de birou / birotica
 25. echipamente tehnologice specifice activitatii
 26. imprimanta/copiator
 27. informatii stocate in sistemul informatic (continand si date cu caracter personal)
 28. informatii stocate pe statiile de lucru din unitate (continand si date cu caracter personal)
 29. instrumentar/vesela
 30. materiale didactice
 31. medicamente
 32. mobilier specific activitatii
 33. numerar
 34. operatiuni curente cu numerar
 35. operatiuni curente fara numerar
 36. operatiuni de securitate
 37. operatiuni informationale
 38. prescolari
 39. personal auxiliar
 40. personal prestatori
 41. seif (dulap de depozitare documente)
 42. server/router
 43. servicii telecomunicatii
-

44. sistem de securitate – interfonie cu control acces
45. sistem securitate - TVCI
46. sistem tehnic de securitate - efracție
47. stație de lucru, desktop, laptop
48. tablou electric general
49. UPS
50. vizitatori / apartinatori

4.4 Analiza de impact

Analiza de impact a fost realizată pe baza criteriilor de determinare a valorii activelor relevante pentru GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA, prezentate mai jos:

Nivel	Nesemnificativ	Minor	Moderat	Major	Catastrofic
Criteriu	A	B	C	D	E
Afectarea sanatații și/sau vieții angajaților, clienților	Nu afectează sănătatea și/sau viața angajaților sau a clienților	Afectarea usoară a sanatații uneia sau mai multor persoane (este suficientă intervenția personalului medical al unității)	Afectarea sanatații angajaților sau clienților fiind necesară intervenția personalului medical de specialitate	Afectarea gravă a sanatații angajaților sau clienților (ranire, intoxicație, spitalizare etc.)	Provocarea decesului angajaților și/sau al clienților
Pierderi legate de întreruperea funcționării	Nu afectează funcționarea în niciun fel	Nu afectează funcționarea datorită rezervelor care intra automat în flux	Nu afectează funcționarea dar reduce drastic nivelul de redundanță și siguranță	Întreruperea de scurtă durată a funcționării (max. 2 ore); poate fi soluționat în timpul respectiv prin resursele	Întreruperea pentru mai mult de 2 ore a funcționării

				interne ale unitatii	
Pierdere financiara directa	Sub 7.500 Euro	Intre 7.501 si 37.500 Euro	Intre 37.501 si 150.000 Euro	Intre 150001 si 1.500.000 Euro	Peste 1.500.000 Euro
Pierdere financiara indirecta	Nesemnificativa	Minora	Moderata	Majora	Critica, poate conduce la incapacitate de functionare
Redundanta/du rata de inlocuire a activului	Exista redundanta sau nu este necesara inlocuirea	Activul poate fi inlocuit imediat (max. 24h)	Activul poate fi inlocuit in termen de cateva zile	Inlocuirea activului se poate face intr-un interval de cateva saptamani	Nu exista redundanta iar inlocuirea activului este inaplicabila
Afectarea imaginii companiei	Fara ecou	Articol in media locala	Articol in media locala si investigatie a autoritatilor locale	Articol in media nationala si investigatii ale autoritatilor locale	Subiect de media de interes pe o perioada de cel putin 3 zile si/sau investigatie a autoritatilor centrale
Pierdere clienti	Nu exista	Sub 2%	intre 2 si 5%	intre 5 si 10%	Peste 10%
Afectarea conformitatii cu prevederile legale, contractuale etc.	Nu afecteaza	Posibil de remediat in timp util pentru a se evita o penalitate	Amenda, plata daune etc. sub 10.000 lei	Penalitati intre 10.001 si 100.000 lei sau contraventie	Penalitati mai mari de 100.001 lei sau infractiune

4.5 Zonarea obiectivului

In conformitate cu legislatia in vigoare si standardele operationale si de securitate ale Nu exista, se evidentiaza urmatoarele zone:

Zona	Descriere
Zona de acces in unitate	<p>ACCES CURTE:</p> <p>Acces auto si pietonal in curte: se realizeaza din Aleea Basmului, prin poarta de acces situata pe latura nordica a obiectivului. Poarta metalica din doua foi cu portita de acces pietonal, inchidere cu lacat, necertificat.</p>  



ACCES GRADINITA: usa de acces din tamplarie de tip PVC cu panouri PVC, din doua canate, necertificata, situata pe latura sudica a cladirii. Usa este prevazuta cu un sistem de interfonie si control al accesului.




ACCES GRADINITA: usa de acces situata pe latura nordica a aripii sudice a cladirii, usa cu tamplarie tip PVC cu geam termopan si panou PVC, necertificata.



	<p>ACCES GRADINITA: usa de acces din tamplarie de tip PVC cu geam termopan si panouri PVC, din doua canate, necertificata, situata pe latura vistica a cladirii.</p>  <p>ACCES CENTRALA TERMICA SI MAGAZIE: Doua usi din tamplarie de tip PVC cu panou PVC, necertificate.</p> 
<p>Zona perimetrala</p>	<p>Imprejmuire realizata cu gard din panouri din beton pe stalpi din beton armat cu inaltimea de 2,20 m.</p> 

	 <p>Curtea interioara a obiectivului.</p>
Zona de tranzactionare numerar	Birou administrator situat la parterul aripii sudice in vecinatatea zonei de acces.
Zona de depozitare numerar	<p>Valorile monetare sunt pastrate pe timpul zilei intr-un dulap de documente certificat antiincendiu, amplasat in biroul administratorului, prevazut cu detector de soc.</p> <p>Dulapul de depozitare documente folosit pentru depozitarea valorilor banesti <u>nu este certificat</u> antiefracție conform SR EN 1143-1:1997/A2.</p> 
Zona de expunere	Nu sunt expuse bunuri pentru vanzare/vizionare
Zona de transfer	Birou administrator - hol acces - usa acces - curte interioara - zona de acces in perimetrul unitatii.
Zona de procesare numerar	Birou administrator situat la parterul aripii sudice in vecinatatea zonei de acces.

Zona echipamentelor de securitate	Birou director si hol zona de acces gradinita din latura sudica.
	
Alte zone cu regim de securitate ridicat	
Sali de clasa	8 sali de clase dispuse la parterul si etajul obiectivului.
Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii	Birouri de contabilitate, administratie, directiune, cabinet medical, izolator, cabinet metodic dispuse la parterul si etajul obiectivului conform ANEXA NR. 8 in urma recompartimentarii obiectivului.
Bloc alimentar	Bucatarie, magazie situat la parterul obiectivului.
Holuri, casele scarilor, coridoare, toalete, vestiar	Situat la parterul si etajul obiectivului conform ANEXA NR. 8 in urma recompartimentarii obiectivului.

<p>Centrala termica</p>	<p>Cladire distincta situata in curtea obiectivului, pe latura vestica.</p> 
-------------------------	--

4.6 Sursele de amenintare

Au fost evaluate amenintarile pornind de la sursele din lista inclusa in metodologia de evaluare a riscurilor la securitatea fizica, fiind considerate relevante:

- autor intern
- autor extern
- hartuitor
- crima organizata
- persoana cu afectiuni psihice
- persoane violente
- terorist
- cutremur
- prabusire structura
- electrocutare
- explozie
- alte accidente
- factor intern/extern
- factor intern

-
- factor extern
 - inundatie
 - intrerupere alimentare cu energie electrica
 - intrerupere comunicatii voce-date
 - persoane nemulumite

4.7 Determinarea si evaluarea amenintarilor la adresa activelor relevante

In Anexa 1 GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA - Active relevante: evaluare impact si surse de amenintare sunt asociate sursele de amenintare relevante cu activele relevante.

Pentru fiecare sursa de amenintare au fost retinute ameninatrile posibile si au fost evaluate scenariile de acces fizic necesar a fi parcurse pentru desfasurarea atacului / actiunii adverse.

Principalele consideratii privind sursele de amenintare includ:

- Unitatea este situata in judetul Bistrita-Nasaud care are un coeficient de criminalitate scazut, in Municipiul Bistrita, care are un coeficient de criminalitate ridicat;
- Unitatea detine numerar;
 - o Depozitare numerar (noaptea): mic < 10000 EUR
 - o Nivel mediu operatiuni cash/zi: mic < 10000 EUR / zi
- Caracteristici locale exterioare: Zona cu trafic pietonal si/sau rutier mediu;
- Accesibilitate: Posibilitate de disimulare/fuga greoaie.

4.8 Enuntarea riscurilor la securitatea fizica

Riscurile la securitatea fizica au fost identificate prin asocierea activelor relevante cu amenintarile generate de sursele de amenintari relevante, iar enuntarea riscurilor respective a fost consemnata prin trei coloane in tabelul riscurilor de securitate fizica din *Anexa 2: GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA - Tabelul riscurilor de securitate fizica* si anume: 'Denumire risc', 'Descriere risc', 'Cauzele riscului'.

Cap. 5. Analizarea riscurilor identificate

5.1 Scenariile de amenintare

Pornind de la activele relevante, zonele de risc in care acestea sunt amplasate, sursele de amenintare relevante si vulnerabilitatile constate, apreciem ca plauzibile urmatoarele scenarii de amenintare:

- Scenariu de 'FURT' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'
- Scenariu de 'DISTRUGERE/VANDALIZARE' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'
- Scenariu de 'TERORISM' in in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'
- Scenariu de 'CUTREMUR' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'
- Scenariu de 'INUNDATIE' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'
- Scenariu de 'ACCIDENTE TEHNOLOGICE' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'

-
- Scenariu de 'AGRESIUNE' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'
 - Scenariu de 'SABOTAJ' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'
 - Scenariu de 'INTRERUPERE ALIMENTARE CU ENERGIE ELECTRICA' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'
 - Scenariu de 'INTRERUPERE ALE RETELELOR DE COMUNICATII' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Holuri, casele scarilor, coridoare'
 - Scenariu de 'RISC IN OPERATIUNILE CU NUMERAR' in 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar'
 - Scenariu de 'RAPIRE SI TRAFIC DE PERSOANE' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar'
 - Scenariu de 'PIERDERE PERSOANE' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de transfer', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar',
 - Scenariu de 'GESTIUNE DEFICITARA' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara'
-

- Scenariu de 'UZ DE DATE CONFIDENTIALE' in 'Zona de acces in unitate', 'Zona perimetrala', 'Zona de tranzactionare numerar', 'Zona de depozitare numerar', 'Zona de transfer', 'Zona de procesare numerar', 'Zona echipamentelor de securitate', 'Sali de clasa', 'Birouri/Oficii/Cabinete de specialitate si incaperi cu alte destinatii', 'Bloc alimentar', 'Curte interioara', 'Holuri, casele scarilor, coridoare, toalete, vestiar', 'Centrala termica'

5.2 Determinarea indicilor de risc

In tabelul riscurilor la securitatea fizica sunt enuntate principalele riscuri de securitate fizica si sunt determinati indicii acestora in baza schemei de determinare a nivelului riscului de securitate fizica din cadrul Metodologiei privind analiza riscurilor de securitate fizica.

Indicele de plauzibilitate a fost determinat prin formula:

$R = P * I$ iar $P = F * V$ unde:

P = plauzibilitate

F = frecventa atacurilor estimata dupa scala din Tabelul 2

Tabelul 2 Scala de frecventa

Indicatori	Scor	Descriere
- este probabil sa nu apara niciodata - frecventa mai mica decat o data la 20 ani	1	improbabil
- poate aparea doar in circumstante profesionale exceptionale - nu este de asteptat sa se intample - nu a fost semnalat in domeniul de activitate - frecventa mai mica de o data la 10 ani	2	foarte putin probabil
- ar putea aparea in anumite circumstante profesionale - se poate intampla ocazional - s-a intamplat in domeniul de activitate - cel putin o data in intervalul de 5 ani	3	posibil
- va aparea probabil in multe circumstante profesionale - se va intampla probabil, dar nu va reprezenta o problema persistenta pentru domeniul de activitate - s-a mai intamplat in trecut - cel putin o data intr-un interval de 2 ani	4	probabil
- este de asteptat sa apara in majoritatea circumstantelor profesionale - se va intampla, eventual frecvent - iminent - frecventa mai mare decat o data in fiecare an	5	aproape sigur

V = coeficient de vulnerabilitate (apreciat de evaluator în urma analizei de securitate) într-o scală de valori întregi de la 1 (invulnerabil, s-au aplicat toate măsurile recomandate de cele mai bune practici) la 5 (total vulnerabil, nu sunt aplicate măsuri de securitate).

Nota: relația dintre variabilele P, F, V este de tipul $P = \text{int}(\sqrt{F \cdot V})$

În Anexa 2 a fost introdusă coloana măsuri de securitate existente care justifică pentru fiecare dintre riscurile identificate, modalitatea prin care măsurile de securitate existente controlează riscul respectiv. În acest sens pot fi bine evidențiate atât frecvența estimată a amenințărilor cât și nivelul de control (sau nivelul de vulnerabilitate) care face ca riscul să rămână în limite acceptabile.

Indicii de risc au fost calculați în conformitate cu Tabelul 3.

Tabelul 3 Schema de determinare a indicelui riscului de securitate fizică

Plauzibilitate (P)		Impact (I)		Risc ($R=f(P, I)$)	
1	improbabil	A	nesemnificativ		
2	foarte puțin probabil	B	minor	Minor	1A, 2A, 3A, 1B, 2B
3	posibil	C	moderat	Moderat	4A, 5A, 3B, 4B, 1C, 2C, 3C, 1D
4	probabil	D	major	Ridicat	5B, 4C, 5C, 2D, 3D, 4D, 1E, 2E
5	aproape sigur	E	foarte semnificativ	Critic	5D, 3E, 4E, 5E

În urma evaluării indicilor de risc a fost completat tabelul din *Anexa 2: GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA - Tabelul riscurilor de securitate fizică*.

Cap. 6. Estimarea riscurilor la securitate fizica

Au fost identificate si evaluate 29 riscuri de securitate fizica.

Dintre acestea:

- 0 riscuri critice;
- 24 riscuri ridicate;
- 5 riscuri moderate;
- 0 riscuri minore.

Criteriile de acceptabilitate sunt urmatoarele:

1. Riscurile peste nivelul Moderat nu sunt acceptabile;
2. Pentru riscurile cu nivelul Moderat se va analiza, de la caz la caz, necesitatea si eficienta tratarii acestora sau monitorizarea lor;
3. Riscurile sub nivelul Moderat pot fi tolerate sau monitorizate, dupa caz.

In conformitate cu criteriile de acceptabilitate se stabileste:

1. Tratarea unui numar de 29 riscuri. Aceste riscuri sunt:
 - 29 riscuri reduse: R0001; R0002; R0003; R0004; R0005; R0006; R0007; R0008; R0009; R0010; R0011; R0012; R0013; R0014; R0015; R0016; R0017; R0018; R0019; R0020; R0021; R0022; R0023; R0024; R0025; R0026; R0027; R0028; R0029;
 - 0 riscuri partajate: -;
 - 0 riscuri evitate: -.
2. Monitorizarea unui numar de 0 riscuri: -.
3. Tolerarea unui numar de 0 riscuri: -.

Mijloacele de control al riscului aplicate fiecarui risc tratat, pentru diminuarea acestora, precum si indicii estimati ai riscurilor reziduale sunt prezentate in Anexa 2.

Cap. 7. Stabilirea cerintelor, masurilor si mecanismelor de securitate pentru sistemul ce urmeaza a fi implementat, de ordin structural, tehnic, tehnologic si operational

La controlul riscurilor la securitatea fizica cu care se confrunta GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA, contribuie urmatoarele:

- atributiile pe linie de securitate inscise in fisa postului angajatilor din unitate si a conducatorilor unitatii;
- masurile tehnice existente;
- implementarea in 60 de zile a recomandarilor prezentului raport:
 - o proceduri si instructiuni de securitate legate de activitatile curente cu publicul, principalele incidente posibile si masurile preventive necesare;
 - o instruirea de securitate realizata periodic pentru a compensa fluctuatia / rotatia personalului;
 - o verificare / audit pentru monitorizarea riscurilor specificate in prezentul raport;
 - o masuri de securitate recomandate.

Sub aspectul legislatiei privind paza obiectivelor, bunurilor si valorilor si protectia persoanelor, autoritatea de reglementare in domeniu (Ministerul de Interne prin Inspectoratul General al Politiei, Directia Ordine Publica) a introdus urmatoarele cerinte de securitate:

HOTARARE Nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor si protectia persoanelor si HOTARAREA Nr. 1002/2015 pentru modificarea si completarea HG Nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor si protectia persoanelor

CAPITOLUL I

Dispozitii generale

Art. 4

Beneficiarii sistemelor avizate sunt obligati sa incheie contracte de intretinere periodica cu societati licentiate, care sa ateste functionarea sistemului conform parametrilor tehnici.

Art. 5

(1) Protectia mecano-fizica cuprinde elementele care asigura delimitarea fizica in scopul protejarii vietii si integritatii personalului operator sau restrictionarii accesului neautorizat la valori.

(2) Gradul de siguranta / rezistenta al elementelor de protectie mecano-fizice utilizate in unitati se stabileste proportional cu cuantumul valorilor protejate si nivelul de risc determinat, recomandandu-se alegerea unei clase de nivel mediu, definita de standardele europene / nationale de profil.

Art. 6

(1) In afara programului de lucru, expunerea bunurilor si valorilor prin intermediul unor suprafete exterioare este permisa doar in situatia in care suprafata vitrata prezinta rezistenta la atacuri

manuale sau se afla in imobile asigurate cu posturi de paza fizica.

(2) Usile si ferestrele exterioare trebuie sa aiba incuietori de siguranta pentru a se asigura intarzierea patrunderii neautorizate in spatiul unitatii, cu exceptia obiectivelor in care este instituita paza fizica si a celor cu program permanent.

(3) Operatiunile cu numerar in zonele de tranzactionare la unitatile financiar-bancare se pot efectua in spatii amenajate, in care personalul este separat de clienti prin elemente de protectie rezistente la actiunea armelor de foc si sertar de preluare indirecta a valorilor, sau prevazute cu seifuri / dulapuri de casierie cu deschidere temporizata ori prin masini de reciclare a numerarului.

(4) Pentru seifurile de depozitare valori monetare care sunt prevazute cu deschidere temporizata, programarea intarzierii la deschidere se face cu timp de cel putin 5 minute. Sunt exceptate seifurile amplasate in zonele de depozitare cu acces temporizat pentru un interval de timp de cel putin 5 minute, precum si seifurile utilizate suplimentar masurilor stabilite prin analiza de risc.

(4) Dulapurile de casierie aflate in spatiile functionale deschise se utilizeaza prin programarea unor timpi de deschidere de minimum 5 minute, pentru sertarul de depozitare a numerarului.*

(5) Automatele bancare, respectiv distribuitorii automate de numerar, masinile de schimb valutar, masinile de reciclat numerar si distribuitorii de numerar destinate casierilor se prevad cu seifuri certificate, cu clasa de rezistenta la efracție determinata si se ancoreaza conform instructiunilor producatorului. Pot fi utilizate si alte solutii tehnice certificate cu rezultate similare sau superioare daca se face dovada caracterului similar sau superior al acestora. In mod similar, seifurile / dulapurile de casierie cu temporizare trebuie sa fie certificate, cu nivel de rezistenta la efracție determinat si se ancoreaza conform instructiunilor producatorului.

Art. 8¹

Unitățile și instituțiile de interes public trebuie să prevadă sisteme de supraveghere video pe căile de acces, holuri și alte zone cu risc ridicat, detecție a efracției pe zonele de expunere sau depozitare valori și control acces prin personal sau echipamente.

CAPITOLUL 5

Art. 68

(1) Sunt supuse avizării poliției proiectele sistemelor de alarmare destinate următoarelor categorii de obiective:

- a) unități de interes strategic și obiective aparținând infrastructurilor critice;*
- b) **unități sau instituții de interes public;***
- c) instituții de creditare, unități poștale, puncte de schimb valutar, case de amanet, unități profilate pe activități cu bijuterii din metale sau pietre prețioase;*
- d) magazine de arme și muniții;*
- e) stații de comercializare a carburanților/combustibililor;*
- f) săli de exploatare a jocurilor de noroc;*
- g) centre de procesare;*
- h) casierii furnizori și servicii de utilități, puncte de colectare ori de depozitare numerar cu plafon de peste 10.000 euro sau echivalent;*
- j) depozite în care se află bunuri cu o valoare mai mare de 10.000 euro sau echivalent.*

Pentru reducerea nivelului de risc de securitate al obiectivului analizat vor fi luate măsuri organizatorice, proceduri de lucru și proceduri de securitate în concordanță cu standardele, normele

și prevederile legale în vigoare, dar **nelimitându-se** la:

- Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor cu modificările și completările ulterioare
- Hotărârea nr. 301 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor publicată în Monitorul Oficial nr. 335 din 17 mai 2012 actualizată cu prevederile Hotărârii Guvernului nr. 1002 din 23 decembrie 2015, publicată în Monitorul Oficial nr. 984 din 30 decembrie 2015
- Instrucțiunea nr. 9 din 1 martie 2013 privind efectuarea analizelor de risc la securitatea fizică a unităților ce fac obiectul Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, cu modificările și completările ulterioare
- Legea 506/2004 și a Legea 272/2006 pentru completarea Legii 506/2004 privind protecția datelor cu caracter personal în comunicațiile electronice;
- Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- Decizia 52/2002 a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal
- Seria de standarde Sisteme de management al calității (SR EN ISO 9001:2008);
- Seria de standarde SR EN 50130 - Sisteme de alarmă. Compatibilitate electromagnetica;
- Seria de standarde SR EN 50131 - Sisteme de alarmă. Sisteme de alarmă împotriva efracției și jafului armat;
- Standardul SR EN 50132-7 - Sisteme de supraveghere TVCI care se utilizează în aplicațiile de securitate; Linii directoare.
- Seria de standarde SR EN 62676 - Sisteme de supraveghere video utilizate în aplicații de securitate;
- Seria de standarde SR EN 50133 - Sisteme de alarmă. Sisteme de control al accesului pentru utilizare în aplicații de securitate;
- Seria de standarde SR EN 50518 - Centru de monitorizare și recepție a alarmelor;
- Standarde europene sau naționale de certificare a mijloacelor de protecție mecano-fizică privind rezistența la efracție sau la glonț:
 - SR EN 356:2003 - Sticlă pentru construcții. Vitraje de securitate. Încercare și clasificare a rezistenței la atacul manual
 - SR EN 1063:2003 Sticlă pentru construcții. Vitraje de securitate. Încercare și clasificare a rezistenței la atacul cu glonț
 - SR EN 1522:2004 Ferestre, uși, obloane și jaluzele. Rezistență la atacul cu glonț. Condiții și clasificare
 - SR EN 1523:2004 Ferestre, uși, obloane și jaluzele. Rezistență la glonț. Metodă de încercare

- SR EN 1047-1:2006 Unități de depozitare de securitate. Clasificare și metode de încercare pentru determinarea rezistenței la foc. Partea 1: Dulapuri pentru date și containere de dischete
- SR EN 1047-2+A1:2013 Unități de depozitare de securitate. Clasificare și metode de încercare pentru determinarea rezistenței la foc. Partea 2: Camere și containere pentru date
- SR EN 1143-1:2012 Unități de depozitare de securitate. Cerințe, clasificare și metode de încercare pentru determinarea rezistenței la efracție. Partea 1: Seifuri, seifuri pentru ATM, uși de tezaur și camere de tezaur
- SR EN 1143-2:2014 Unități de depozitare de securitate. Cerințe, clasificare și metode de încercare pentru determinarea rezistenței la efracție. Partea 2: Sisteme de depunere
- SR EN 1300:2014 Unități de depozitare de securitate. Clasificarea încuietorilor de înaltă securitate în funcție de rezistența la efracție
- SR EN 14450:2005 Unități de depozitare de securitate. Cerințe, clasificare și metode de încercare pentru determinarea rezistenței la efracție. Dulapuri de securitate
- SR EN 1627:2011 Uși pentru pietoni, ferestre, fațade cortină, grilaje și obloane. Rezistență la efracție. Cerințe și clasificare
- SR EN 1628:2011 Uși pentru pietoni, ferestre, fațade cortină, grilaje și obloane. Rezistență la efracție. Metodă de încercare pentru determinarea rezistenței la solicitare statică
- SR EN 1629:2011 Uși pentru pietoni, ferestre, pereți cortină, grilaje și obloane. Rezistență la efracție. Metodă de încercare pentru determinarea rezistenței la solicitare dinamică
- SR EN 1630:2011 Uși pentru pietoni, ferestre, fațade cortină, grilaje și obloane. Rezistență la efracție. Metodă de încercare pentru determinarea rezistenței la tentative manuale de efracție

În concluzie, pentru completarea măsurilor existente la GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA pentru a asigura conformitatea cu prevederile legale sunt necesare măsuri de remediere prezentate în continuare.

În conformitate cu rezultatele analizei de riscuri și în baza prevederilor HG nr.301/2012 și HG nr.1002/2015, principalele componente tehnice necesare pentru diminuare riscurilor 'critic' și 'ridicat' sunt prezentate în tabelul de mai jos.

Măsurile propuse se vor implementa ca urmare a proiectului de modernizare a unității.

Tabelul 4 Măsuri propuse

Nr.	Măsura	Descriere
1	Subsistem de alarmare la efracție	În urma modificărilor și a modernizării unității se va instala un sistem de alarmare la efracție care să asigure detectia patrunderii prin efracție cel puțin în următoarele zone:

		<p>-zonele de acces in cladire</p> <p>-zona de tranzactionare</p> <p>-zona de depozitare</p> <p>-zona de transfer (toate incaperile de la nivelul parter, holurile, coridoarele si casele scarilor de la parter;</p> <p>- alte zone cu regim de securitate ridicat: holurile, coridoarele si casele scarilor de la etaj, incaperile de la etaj: arhiva, contabilitate, administratie, magazine, cabinete, directiune, centrala termica.</p> <p>Centrala sistemului de alarmare la efracție se va amplasa într-o incapere distincta cu acces restrictionat.</p> <p>Se va asigura posibilitatea armarii partitionate in incaperile in care nu exista program prelungit (birouri, arhiva, magazine, cabinete, directiune).</p> <p>Tastatura sistemului se va amplasa in vecinatatea zonei de acces principal in cladire.</p> <p>Sirena de exterior se va amplasa pe fatada adiacenta celei mai circulat strazi.</p>
2	Semnalizare stare de pericol personal	Se vor instala dispozitive de semnalizare a starii de pericol ("butoane/pedala panica") asupra personalului cel putin in urmatoarele zone: birou administrator, birou director.
3	Seif ancorat si protejat cu detector de vibratii	Se va instala un seif certificat antiefracție in conformitate cu SR EN 1143-1:1997/A2, se va ancora conform instructiunilor producatorului si se va proteja antiefracție cu un detector de vibratii conectat pe zona distincta a sistemului de alarmare la efracție.
4	Conectare la dispecerat de monitorizare	Sistemul de alarmare la efracție va fi conectat la un dispecerat de monitorizare.
5	Utilizare back-up comunicatii securitate in alt mediu tehnic decat cel de baza	Asigurarea transmisiei la distanta a evenimentelor legate de sistemele de securitate in cel putin doua medii de transmisie (ex. linie telefonica fixa si GSM/GPRS) catre dispeceratul de monitorizare.
6	Interventie prin personal specializat	Interventie la evenimentele privind securitatea obiectivului cu personal specializat.

7	Sistem supraveghere video TVCI	<p>Se va instala un sistem de supraveghere video care sa permita preluare de imagini cel putin din urmatoarele zone:</p> <ul style="list-style-type: none"> -zonele de acces in unitate -zona perimetrala a unitatii (curtea interioara) -zonele de transfer (holurile, coridoarele si casele scarilor) -zona de depozitare (seiful) <p>Alte zone cu regim de securitate ridicat:</p> <ul style="list-style-type: none"> -zona centralei termice -zona de acces in incaperea care va adaposti echipamentele de securitate si seiful. <p>Dispozitivul de inregistrare, sursele de alimentare, UPS-ul se vor amplasa intr-o incapere distincta cu acces restrictionat.</p>
8	Asigurarea calitatii imaginilor care sa permita recunoasterea persoanelor ce acced in unitate	<p>Pentru zonele: poarta de acces in perimetrul unitatii si punctele de acces in cladire, camerele de supraveghere video trebuie sa asigure calitatea imaginii care sa permita recunoasterea persoanelor care acced in unitate conform EN 62676.</p>
9	Asigurarea stocarii imaginilor video pentru 20 zile	<p>Dispozitivul de inregistrare se va dota cu unitati de stocare (HDD) care sa asigure stocarea imaginilor pe cel putin 20 de zile la calitatea impusa.</p> <p>Se va asigura si verifica in permanenta daca imaginile stocate pe dispozitivele de inregistrare sunt pastrate pentru minim 20 zile.</p>
10	UPS sistem supraveghere video	<p>Sistemul de supraveghere video TVCI se va dota cu o sursa neintreruptibila (UPS) care sa asigure functionarea sistemului in cazul intreruperii alimentarii cu energie electrica de la sursa de baza pentru cel putin 15 minute.</p> <p>Se va asigura si verifica in permanenta starea de functionare a UPS – ului.</p>
11	Sistem de control al accesului persoanelor	<p>Se va implementa un sistem de control acces care sa asigure deschiderea controlata a portii pietonale si a usilor de acces in cladire.</p> <p>Poarta de acces in curtea unitatii se va mentine permanent inchisa si asigurata.</p>

12	Revizia sistemului tehnic de securitate	Realizarea de operatiuni de testare a functionarii, verificare si mentinere in buna stare de functionare a sistemelor instalate pe baza unui contract de mentenanta, cel putin odata la semestru si consemnarea acestora in documentele specifice (JURNAL SISTEM TEHNIC DE SECURITATE).
13	Proceduri de securitate	<p>Elaborarea de proceduri de securitate prin care sa se realizeze instruirea personalului cu privire la accesul si parasirea obiectivului, identificarea si inregistrarea vizitatorilor si a colaboratorilor, utilizarea echipamentelor de securitate, modul de actiune la producerea unui incident de securitate.</p> <p>Informarea, instruirea si testarea personalului privind politicile si procedurile securitate si practicile de lucru in conditii de siguranta. Instruirea personalului privind accesul in incinta, apropierea sau prezenta unor persoane sau obiecte suspecte, primirea coletelor sau plicurilor suspecte.</p> <p>Proceduri privind selectia si testarea periodica a personalului propriu.</p> <p>Proceduri de selectie a furnizorilor si a colaboratorilor.</p> <p>Proceduri interne privind procesarea, depozitarea respectiv transportul valorilor.</p> <p>Respectarea procedurilor specifice activitatii.</p> <p>Respectarea procedurilor privind predarea si preluarea prescolarilor.</p>
14	Instruirea personalului cu privire la procedurile de lucru de securitate	Instruirea si asumarea de catre personal a procedurilor de securitate elaborate.
15	Intocmirea si avizarea proiectului sistemului tehnic de securitate	Elaborarea proiectului tehnic al sistemului de alarmare in caz de efracție si supraveghere video conform Anexei 7 la HG 301/2012 actualizata conform HG1002/2015, in vederea avizarii de catre IPJ.
16	Proceduri de gestionare a conflictelor	Elaborarea de proceduri de lucru privind mamagementul conflictelor.
17	Proceduri SSM/SU	Respectarea procedurilor de securitate si sanatare in munca si a procedurilor de actiune in

		situatii de urgenta.
18	Usi si ferestre certificate	La inlocuirea tamplariei se va acorda atentie la folosirea usilor cu tamplarie rezistenta la efracție, incuietori certificate antiefracție si ferestre rezistente la efracție avand deschidere limitata.
19	Inlocuire gard	Imprejmuirea unitatii cu un gard cu inaltimea minima de 2,20, astfel incat acesta sa nu reprezinte un pericol la adresa integritatii fizice a prescolarilor.

Suplimentar, în vederea asigurării unei securități sporite a persoanelor și bunurilor din obiectiv, sunt necesare următoarele măsuri:

- 1. Desemnarea a unui coordonator pe probleme de securitate si delegarea sarcinilor privind securitatea fizica a obiectivului catre responsabili – persoane stabilite – din fiecare schimb (tura)*
- 2. Inainte de inchiderea spatiilor in care nu exista serviciu prelungit se vor verifica toate incaperile pentru a nu ramane persoane in interior.*
- 3. La parasirea obiectivului se vor verifica toate incaperile pentru a nu ramane persoane in interior.*
- 4. Colaborarea cu alte structuri cu responsabilitati in paza bunurilor si ordinea publica*

Cap. 8. Estimarea costurilor de securitate in functie de masurile de securitate propuse si nivelul de risc asumat

Implementarea mijloacelor de control al riscurilor mentionate la capitolul 7 se poate face prin parcurgerea unei etape de proiectare (studiu de fezabilitate, proiect tehnic si elaborare caiete de sarcini), etapa in urma careia se poate determina valoarea de investitie necesara. Costurile estimate ale masurilor de securitate propuse pentru incadrarea obiectivului in limitele de risc asumate sunt prezentate in tabelul de mai jos.

Tabelul 5 Masuri propuse si costurile estimate

Nr.	Masura	COST EURO
1	Subsistem de alarmare la efracție	2500 - 3000
2	Semnalizare stare de pericol personal	150
3	Seif ancorat si protejat cu detector de vibratii	400-600
4	Conectare la dispecerat de monitorizare	250 – 350 ANUAL
5	Utilizare back-up comunicatii securitate in alt mediu tehnic decat cel de baza	100 – 200
6	Interventie prin personal specializat	Inclus in costul monitorizarii
7	Sistem supraveghere video TVCI	2500 - 4000
8	Asigurarea calitatii imaginilor care sa permita recunoasterea persoanelor ce acced in unitate	Inclus in costul sistemului TVCI
9	Asigurarea stocarii imaginilor video pentru 20 zile	Inclus in costul sistemului TVCI
10	UPS sistem supraveghere video	300 – 400
11	Sistem de control al accesului persoanelor	1500 - 2000
12	Revizia sistemului tehnic de securitate	400 – 500 ANUAL
13	Proceduri de securitate	Cost intern
14	Instruirea personalului cu privire la procedurile de lucru de securitate	Cost intern
15	Intocmirea si avizarea proiectului sistemului tehnic de securitate	600 - 1000
16	Proceduri de gestionare a conflictelor	Cost intern
17	Proceduri SSM/SU	Cost intern
18	Usi si ferestre certificate	Inclus in costul proiectului de modernizare
19	Inlocuire gard	Inclus in costul proiectului de modernizare

Cap. 9. Concluzii

Evaluarea riscurilor de securitate fizica la GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA a fost efectuată în perioada **11.05.2021 – 14.05.2021.**, de către o echipă coordonată de ERSF TOTH MÁRTON în colaborare cu coordonatorul pe probleme de securitate al beneficiarului.

Conform HG nr.301/2012 și HG 1002/2015 obiectivul GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA se încadrează în clasa

UNITATI DE INTERES PUBLIC.

Au fost identificate un număr de 50 active relevante și evaluate un număr de 19 surse de amenințare.

Au fost reținute un număr de 29 riscuri de securitate fizica relevante pentru care au fost evaluate următoarele niveluri de risc:

- riscuri critice: 0;
- riscuri ridicate: 24;
- riscuri moderate: 5;
- riscuri minore: 0.

Au fost propuse mijloace de reducere pentru un număr de 29 riscuri.

Situația evaluată a riscurilor reziduale, în număr de 29 fiind:

- riscuri critice: 0;
- riscuri ridicate: 0;
- riscuri moderate: 9;
- riscuri minore: 20.

Evaluatorul recomandă monitorizarea unui număr de 0 riscuri: -, pentru care există suficiente măsuri de securitate aplicate, dar care pot spori în efectivitate prin adaptare continuă la diversitatea formelor de manifestare a riscurilor.

Măsurile existente și aplicarea măsurilor recomandate asigură încadrarea riscului în limita reglementată în conformitate cu grila de evaluare anexată. Scorul total final al grilei de evaluare este:

57.375 % - Grila de evaluare este prezentată anexat

Nivelurile acceptabile au fost calculate astfel:

- Folosind elemente de evaluare cu **efect de diminuare a riscului având impact SEMNIFICATIV** (total 7 puncte), luând în considerare următoarele elemente:

-
- imprejmuire cu gard – 3 punct
 - semnalistica privind existenta sistemelor de securitate – 2 puncte
 - acces cu deschidere controlata din interior – 2 puncte.

DOCUMENTE ADITIONALE ANEXATE LA RAPORT:

<i>Documentul</i>		<i>Nr. file</i>
Anexa 1	<i>Active relevante</i>	3
Anexa 2	<i>Tabelul riscurilor de securitate fizica</i>	6
Anexa 3	<i>Diagrama plauzabilitate</i>	1
Anexa 4	<i>Decizie Consiliul popular al jud. Bistrita-Nasaud</i>	1
Anexa 5	<i>Hotarare Consiliul local al Mun. Bistrita</i>	6
Anexa 6	<i>Coeficienti criminalitate la nivel de judet</i>	2
Anexa 7	<i>Coeficienti criminalitate la nivel de localitate</i>	2
Anexa 8	<i>Planuri de situatie</i>	3
Anexa 9	<i>Organigrama</i>	1
Anexa 10	<i>Contract mentenanta sistem de securitate</i>	1
Anexa 11	<i>Contract de monitorizare si interventie</i>	1
Anexa 12	<i>Formular culegere date</i>	8
Anexa 13	<i>Certificat de atestare fiscala</i>	1
Anexa 14	<i>Certificat de inregistrare fiscala</i>	1
Anexa 15	<i>Extras CF</i>	3

Prezentul raport a fost intocmit pornind de la analiza situatiei de fapt din obiectivul GRADINITA CU PROGRAM PRELUNGIT NR. 13 - BISTRITA, a masurilor de securitate existente, a vulnerabilitatilor si a riscurilor la securitatea fizica. Masurile de securitate propuse urmaresc sa asigure un raport cost - beneficiu optim si incadrarea obiectivului intr-un nivel de risc acceptabil conform cerintelor legale in vigoare. Beneficiarul are obligatia punerii in aplicare a masurilor de securitate propuse in termen de 60 de zile de la asumarea prezentului raport, potrivit art. 4, alineatul 2 din *INSTRUCTIUNILE nr. 9 din 1 martie 2013 privind efectuarea analizelor de risc la securitatea fizica a unitatilor ce fac obiectul Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor si protectia persoanelor*.

Conform standardului EN31000, optiunile de tratare a riscurilor nu sunt neaparat exclusive sau potrivite in orice circumstante. Optiunile de tratare a riscurilor pot include si:

- Decizia de a nu porni sau de a nu continua activitatea generatoare de risc
- Asumarea sau cresterea expunerii la risc in scopul atingerii unui scop
- Indepartarea sursei generatoare de risc
- Mentinerea riscului pe baza unei decizii in cunostinta de cauza.

Totodata, implementarea celor mai potrivite optiuni de tratare a riscurilor implica ponderarea

(echilibrarea) costurilor si eforturilor de implementare, pe de o parte, cu beneficiile ce se obtin, pe de alta parte, avand in vedere prevederile legale, regulamentele si alte cerinte, cum ar fi responsabilitatea sociala sau protectia mediului inconjurator.

TOTH MÁRTON

Nr. Inreg. RNERSF: 413/22.12.2014

**AM LUAT LA CUNOSTINTA CONTINUTUL MATERIALULUI DE FATA, INTELEG
ROLUL SI IMPORTANTA MASURILOR PREVAZUTE, DREPT CARE SEMNEZ
(reprezentantul unitatii evaluate)**