

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი

სამაგისტრო ნაშრომი

გურამ ოთარაშვილი

ფიზიკური უსაფრთხოება და მისი მხარდაჭერა

სამაგისტრო პროგრამა: ინფორმაციული ტექნოლოგიები

ნაშრომი შესრულებულია ინფორმაციული ტექნოლოგიების მაგისტრის აკადემიური
ხარისხის მოსაპოვებლად

ხელმძღვანელი: ტექ. მეცნ. კანდ. გელა ბესიაშვილი

თბილისი

2014 წელი

სარჩევი

ანოტაცია	4
1. გავრცელების არეალი (SCOPE).....	6
2. უსაფრთხოების რისკების შეფასება	6
3. ფიზიკური უსაფრთხოების რისკების მოპყრობა	7
4. პოლიტიკის პერიოდული განხილვა	8
5. კოლექტივი/პერსონალი.....	10
5.1 დაცვა	10
5.2 ვიზიტორები	12
6. გარე პერიმეტრი	13
6.1 შენობის გარე სტრუქტურა	13
6.2 შენობაში შესასვლელი და გასასვლელი წერტილები.....	14
6.3 შენობის კედლები, ფანჯრები და კარები.....	14
6.4 შენობის პერიმეტრის უსაფრთხოება.....	15
6.5 საავარიო გასასვლელები.....	15
6.6 გარე განათება.....	16
6.7 სახურავის უსაფრთხოება	16
6.8 გარე პერიმეტრის კონტროლის კამერები	17
7. ოფისის არე/მიმღები არე	17
8. მაღალი უსაფრთხოების არეალი.....	18
8.1 უსაფრთხოების კონტროლის ოთახი.....	18
8.2 უსაფრთხოების დაცვა და წვდომის პროცედურები.....	20
8.3 ოთახები	21

8.4	საცავი.....	21
8.5	შიდა უსაფრთხოება	22
8.6	განგაშის სისტემები და ღილაკები	23
8.7	საკეტები და გასაღებები.....	24
8.8	შიდა პერიმეტრის კონტორლის კამერები	25
8.9	უსაფრთხოების მოწყობილობების ინსპექტირება	27
8.10	აპარატურის განლაგება და დაცვა.....	28
	დასკვნა.....	29
	გამოყენებული ლიტერატურა.....	30

ანოტაცია

წარმოდგენილი სამაგისტრო ნაშრომი ეძღვნება ფიზიკური უსაფრთხოების და მისი მხარდაჭერის საკითხებს. განხილულია ინფორმაციულ ტექნოლოგიებზე დაფუძნებული ტექნიკური საშუალებები, რომლებიც უზრუნველყოფენ ფიზიკურ უსაფრთხოებას, როგორც შენობაში, ასევე მის გარშემო არსებულ პერიმეტრზე. აღწერილია რისკები, რომლებიც შესაძლებელია არსებობდეს ამ კუთხით. ასევე გაანალიზებულია ამ რისკების აღმოჩენის და აღმოფხვრის გამოყენებადი თანამედროვე ტექნოლოგიური საშუალებები. ძირითადი ყურადღება გამახვილებულია იმ ტექნიკურ საშუალებებზე, რომლებიც დაკავშირებულია ინფორმაციულ ტექნოლოგიებთან. შეფასებები წარმოდგენილია რეკომდებების სახით.

Annotation

The master thesis is devoted to physical security and its support issues. Information technology based technical resources, which ensure the physical security of the building and its surrounding perimeter, are discussed. Risks that may exist in this regard are described and modern technological tools used to identify and eliminate / reduce given risks are analyzed. The main focus is on the technical solutions related to information technology. Estimates are presented in the form of recommendations.

შესავალი

ინფორმაციული უსაფრთხოების ერთ-ერთ უმნიშვნელოვანეს ასპექტს წარმოადგენს ფიზიკური უსაფრთხოება. უსაფრთხოება, რომელიც ტექნიკური საშუალებებით მიიღწევა, შეზღუდულია და მისი მხარდაჭერა უნდა მოხდეს შესაბამისი მენეჯმენტისა და პროცედურების მეშვეობით. სასურველი და საჭირო კონტროლის მექანიზმების გამოვლენა მოითხოვს ფრთხილ დაგეგმვას დეტალების გათვალისწინებით. ფიზიკური უსაფრთხოების მართვა მოითხოვს ყველა თანამშრომლის თანამონაწილეობას. ამის გარდა, იგი შესაძლოა მოითხოვდეს დაინტერესებული წრეების, მომწოდებლების, მესამე მხარის, მომხმარებლების ან გარე მხარეების მონაწილეობას. შესაძლოა ასევე აუცილებელი გახდეს გარედან მოწვეული სპეციალისტის რჩევა.

ინფორმაცია ორგანიზაციისთვის ისეთივე არსებითი აქტივია, როგორც საქმიანობის მართვის სხვა მნიშვნელოვანი აქტივები და მას შესაბამისი დაცვა სჭირდება. ეს საკითხი განსაკუთრებით აქტუალური ხდება ურთიერთდამოკიდებულ და დაკავშირებულ ბიზნეს-გარემოში, რასაც შედეგად მოსდევს სისუსტეებისა და საფრთხეების მზარდი რაოდენობის მიმართ ინფორმაციის დაუცველობა.

ინფორმაციული უსაფრთხოება მიიღწევა შესაბამისი კონტროლის მექანიზმების, მათ შორის პოლიტიკების, პროცესების, პროცედურების, ორგანიზაციული სტრუქტურისა და პროგრამული უზრუნველყოფისა, აგრეთვე კომპიუტერული ტექნიკის დანერგვით. უნდა მოხდეს აღნიშნული კონტროლის მექანიზმების ჩამოყალიბება, დანერგვა, მონიტორინგი, გადახედვა და საჭიროების შემთხვევაში, გაუმჯობესება, რათა ამით უზრუნველყოფილი იყოს ორგანიზაციისთვის მნიშვნელოვანი ბიზნეს-მიზნების მიღწევა და დაცვა. ინფორმაციული უსაფრთხოების სისტემა უნდა დაინერგოს და ფუნქციონირებდეს საქმიანობის მართვის სხვა პროცესებთან ერთად.

ინფორმაციული უსაფრთხოება მნიშვნელოვანია როგორც საჯარო, ასევე კერძო სექტორის საქმიანობისთვის, აგრეთვე კრიტიკული ინფრასტრუქტურის დაცვისათვის. ინფორმაციული უსაფრთხოება ორივე სექტორში შუამავლის ფუნქციას ასრულებს, მაგალითად, ის გამოიყენება ელექტრონული მმართველობის, ან ელექტრონული ბიზნესის (საქამისწარმოების) მიზნების მისაღწევად, ასევე ამ პროცესებთან დაკავშირებული რისკების შესამცირებლად ან თავიდან ასარიდებლად. საჯარო და კერძო ქსელების ურთიერთდაკავშირება და ინფორმაციული რესურსების გაზიარება ართულებს წვდომის

კონტროლის მექანიზმების დანერგვასა და მისი მიზნების მიღწევას. მონაცემების განაწილებულმა დამუშავებამ ასევე შეასუსტა კონტროლის ძირითადი მექანიზმები.

1. გავრცელების არეალი (SCOPE)

მოცემული ნაშრომი წარმოადგენს სახელმძღვანელო მითითებებსა და ზოგად პრინციპებს ორგანიზაციაში ფიზიკური ინფორმაციული უსაფრთხოების მართვის და უზრუნველყოფის(დანერგვის, მხარდაჭერისა, გაუმჯობესებისთვის) შესახებ.

დოკუმენტში წარმოდგენილი კონტროლის მიზნებისა და კონტროლის მექანიზმების ამოცანაა მათი დანერგვა მოხდეს შეფასებული რისკების შედეგად გამოვლენილი მოთხოვნების დაკმაყოფილებისთვის. მოცემული დოკუმენტი შეიძლება გამოყენებული იქნას, როგორც ორგანიზაციული ფიზიკური უსაფრთხოების სტანდარტის და ფიზიკური უსაფრთხოების ეფექტიანი მართვის წესების შემუშავების პრაქტიკული სახელმძღვანელო.

2. უსაფრთხოების რისკების შეფასება

ორგანიზაციის მიზნებიდან გამომდინარე რისკების შეფასების შედეგად უნდა გამოვლინდეს, რაოდენობრივად შეფასდეს და განისაზღვროს რისკების პრიორიტეტი.. შედეგებმა უნდა განსაზღვროს მენეჯმენტის ის შესაძლო ქმედებები და პრიორიტეტები კონტროლის მექანიზმების დანერგვის პროცესში, რომლებმაც ორგანიზაცია ფიზიკური უსაფრთხოების რისკებისგან უნდა დაიცვან. რისკების შეფასების და კონტროლის პროცესი შესაძლოა განხორციელდეს რამდენჯერმე, რათა დაიცვას ორგანიზაციის სხვადასხვა მიმართულებები, ან საინფორმაციო სისტემები.

რისკის შეფასება უნდა შეიცავდეს სისტემურ მიდგომას. საჭიროა ფასდებოდეს რისკის მაგნიტუდა (რისკების ანალიზი) და ხორციელდებოდეს მათი შედარება რისკების შეფასების კრიტერიუმთან, რათა მოხდეს რისკის მნიშვნელოვნების დადგენა (რისკის დონის დადგენა).

რისკების შეფასებები უნდა ხორციელდებოდეს პერიოდულად, რათა შეფასების დროს აისახოს მომხდარი ცვლილებები. მაგალითად, უნდა შეფასდეს აქტივები, საფრთხეები,

სისუსტეები, რისკის ზემოქმედება. უნდა დადგინდეს რისკის დონე იმ შემთხვევებისთვის, როდესაც ხორციელდება მნიშვნელოვანი ცვლილებები. რისკების შეფასება უნდა განხორციელდეს იმ მეთოდური მიდგომით, რომლებიც შედარებად შედეგებს იძლევა.

ორგანიზაციის ფიზიკური უსაფრთხოების რისკის შეფასებას უნდა გააჩნდეს მკაფიოდ დადგენილი ფარგლები, იმისათვის, რომ იყოს ეფექტიანი და ჰქონდეს კავშირი სხვა სფეროებში ჩატარებულ რისკების შეფასებებებთან(საჭიროების შემთხვევაში).

რისკების შეფასება შეიძლება განხორციელდეს მთელი ორგანიზაციის მასშტაბით, მოიცავდეს ორგანიზაციის ნაწილს, ინდივიდუალურ აქტივს, კონკრეტული სისტემის კომპონენტებს, ან რომლიმე სერვისს. რისკების შეფასება საჭიროა ყველგან, სადაც ეს შესაძლებელია, პრაქტიკულია და გამოსადეგარია.

3. ფიზიკური უსაფრთხოების რისკების მოპყრობა

რისკებთან მოპყრობის დაწყებამდე, ორგანიზაციამ უნდა განსაზღვროს რისკების მისაღებობის კრიტერიუმები. რისკი შეიძლება იყოს მიღებული, თუ, მაგალითად, მის მიერ მიყენებული პოტენციური ზარალი არის მცირე, ან მასთან მოპყრობის დანახრჯი არ არის მისაღები. ყოველი მსაგვსი გადაწყვეტულება უნდა იყოს აღწერილი და დოკუმენტირებული.

თითოეული იდენტიფიცირებული რისკითვის, მათი შეფასების შესაბამისად უნდა განხორციელდეს გარკვეული რეაგირება. რისკზე რეაგირება და მასთან მოპყრობა შესაძლოა მოიცავდეს შემდეგ ვარიანტებს:

1. კონტროლის მექანიზმების დანერგვა რისკის შესამცირებლად;
2. რისკის მიღება შეგნებულად და ობიექტურად, რაც ნათლად და ცალსახად შეესაბამება ორგანიზაციის პოლიტიკას, მიზნებს და რისკის მიღების კრიტერიუმს;
3. რისკების თავიდან აცილება, მათი გამომწვევი მოვლენების არდაშვების შედეგად;
4. რისკების გადაცემა ასოცირებული მხარეებისათვის, მაგალითად სადაზღვევო, სერვისების მომწოდებელი, ან სხვა ორგანიზაციებისთვის.

იმ რისკებისთვის, რომელთა მოპყრობის გადაწყვეტილება იქნა მიღებული, უნდა დაინერგოს სათანადო კონტროლის მექანიზმები. ეს კონტროლის მექანიზმები უნდა შეირჩეს და დაინერგოს რისკების შეფასების მოთხოვნების შესაბამისად.

კონტროლის მექანიზმები

კონტროლის მექანიზმმა უნდა უზრუნველყოს რისკების მისაღებ დონეზე შემცირდება შემდეგის გათვალისწინებით:

1. ეროვნული და საერთაშორისო საკონონმდებლო მოთხოვნები და რეგულაციები;
2. ორგანიზაციული მიზნები;
3. საოპერაციო მოთხოვნები;
4. დანერგვისა და ფუნქციონირების ხარჯები, რაც დაკავშირებულია შესამცირებელ რისკებთან და არის ორგანიზაციის მოთხოვნების პროპორციული;
5. უსაფრთხოების ჩავარდნებიდან გამომდინარე სავარაუდო ზიანის შესაბამისად კონტროლის მექანიზმების დანერგვისა და ფუნქციონირებისთვის ინვესტიციების დაბალანსების საჭიროება.

4. პოლიტიკის პერიოდული განხილვა

ფიზიკური უსაფრთხოების კონტროლისთვის უნდა განისაზღვროს პასუხისმგებელი პირი (მფლობელი), რომელიც ამტკიცებს მენეჯმენტის პასუხისმგებლობას უსაფრთხოების გეგმის შემუშავებაზე, განხილვასა და შეფასებაზე. განხილვა უნდა მოიცავდეს ორგანიზაციის ფიზიკური უსაფრთხოების სტრუქტურის გაუმჯობესების შესაძლებლობებს და ინფორმაციული უსაფრთხოების მართვისადმი მიდგომის ორგანიზაციული გარემოს, ბიზნესის ვითარებების, ან ტექნიკური გარემოს ცვლილებების საპასუხოდ.

უსაფრთხოების სტრუქტურის განხილვის დროს გათვალისწინებული უნდა იყოს მენეჯმენტის მიერ ჩატარებული განხილვების შედეგები. უნდა განისაზღვროს მენეჯმენტის მხრიდან ჩასატარებელი განხილვების პროცედურები, მათ შორის განხილვების პერიოდულობა ან განრიგი.

მენეჯმენტის მხრიდან ჩასატარებელი განხილვების საგანი უნდა მოიცავდეს შემდეგ საკითხებს:

- პრევენციული და მაკორექტირებელი ქმედებების სტატუსი
- წინა მენეჯერული განხილვების შედეგები(თუ არსებობს ესეთი);
- პროცესის წარმადობის მაჩვენებლები და ფიზიკური უსაფრთხოების პოლიტიკის შესაბამისობა;

- ცვლილებები, რომლებმაც შესაძლოა გავლენა იქონიონ ორგანიზაციის მიდგომაზე ფიზიკური უსაფრთხოების მართვისადმი.

- საფრთხეებსა და სისუსტეებთან დაკავშირებული ტენდენციები;
- ანგარიშგებები ფიზიკური უსაფრთხოების ინციდენტების შესახებ;
- შესაბამისი უფლებამოსილი პირების მიერ გამოცემული რეკომენდაციები.

მენეჯმენტის მიერ ჩატარებული განხილვის შედეგები უნდა მოიცავდეს შემდეგ საკითხებთან დაკავშირებულ გადაწყვეტილებებსა და ქმედებებს:

1. ფიზიკური უსაფრთხოების მართვისადმი ორგანიზაციის მიდგომის და მისი პროცესების გაუმჯობესება;
2. კონტროლის მიზნებისა და მექანიზმების გაუმჯობესება;
3. რესურსებისა და/ან პასუხისმგებლობების განაწილების გაუმჯობესება.

მენეჯმენტის მხრიდან ჩატარებული განხილვების შესახებ უნდა გაკეთდეს შესაბამისი ჩანაწერები.

მენეჯმენტის მხრიდან საჭიროა ჩასწორებული პოლიტიკის დამტკიცება.

ფიზიკური უსაფრთხოება:

ზოგადად და მიღებულია, რომ ფიზიკური გარემოს დაყოფა ხდება ოთხ ძირითად ნაწილად. ესენია კოლექტივი/პერსონალი, გარე პერიმეტრი, ოფისის და მიმღები არე და მაღალი უსაფრთხოების არე.

თითოეული ზემოთ აღნიშნული არე საჭიროებს, შესაბამისი კონტროლების დანერგვას ფიზიკური უსაფრთხოების უზრუნველსაყოფად. წარმოგიდგენთ თითოეული თავის განხილვას ფიზიკური უსაფრთხოების ჩარჩოების ფარგლებში.

5. კოლექტივი/პერსონალი

5.1 დაცვა

5.1.1 წინასწარი შერჩევა

ორგანიზაციაში არსებული ან ვენდორისგან დაქირავებული უსაფრთხოების ოფიცრები უნდა აკმაყოფილებდეს წინასწარ შედგენილ და დამტკიცებულ საკვალიფიკაციო სკრინინგ მოთხოვნებს, რადგან ზუსტად ესეთ საკვანძო წერტილებზეა დამოკიდებული მაღალი უსაფრთხოების არის მუშაობა(HSA), რომელიც პირდაპირ პროპორციულად ასახავს შემდგომში გამოვლენილ შედეგებს. ამასთანავე ამ ტიპის მომსახურების გამწვევი ვენდორი პასუხისმგებლობას უნდა იღებდეს მომავალში არსებულ შესაძლო დანაკარგებზე და ხარვეზებზე.

დაცვას არ უნდა ქონდეს ავტორიზებული წვდომის უფლება ისეთ სენტიურ მართვის კომპონენტებზე და ოთახებზე, როგორებიც არის:

- მაღალი უსაფრთხოების არე HSA
- თანამშრონლების პირადი ჩანაწერები
- აუდიტის ჩანაწერები

ასევე დაცვას კატეგორიულად აკრძალული უნდა ქონდეს, რაიმე სახით შიდა სისტემების კომფიგურაციის მოდიფიცირება, ცვლილება ან განადგურება. ეს შეეხება უსაფრთხოების მაფრთხილებელ სისტემებს (ეგრედწოდებული AlarmSystems) და ჩანაწერების(ვიდეო, ფოტო და სისტემური ჩანაწერები) შემნახველ მოწობილობებს.

5.1.2 წესები და პასუხისმგებლობა

დაცვის ძირითადი ვალდებულებაა და მთავარი როლია, რომ მან მაღალ დონეზე აკონტროლოს პერიმეტრზე არსებული უსაფრთხოების წერტილები(როგორც მინიმუმ სამუშაო საათებში). მან უნდა უზრუნველყოს შენობის(ების) უსაფრთხოება, არაავტორიზებული ფიზიკური წვდომის პრევენცია, პერსონალის ფიზიკური უსაფრთხოების უზრუნველყოფა და რაიმე უსაფრთხოების პარამეტრის დარღვევის შემთხვევაში, მან დაუყოვნებლივ უნდა აცნობოს შესაბამისად ორგანიზაციის მმართველ ორგანოს, რადგან მიღებულ იქნას ადეკვატური გადაწყვეტილება არსებული ხარვეზის

ბოლომდე გამოსავლენად და მის აღმოსაფხვრელად. ამასთან დაკავშირებით უსაფრთხოების ვენდორმა უნდა უზრუნველყოს შემდეგი ასპექტები:

- რომ დაცვის თანამშრომლები ინარჩუნებენ თავისი მოვალეობების პირნათლად შესრულებას და ასევე ინაწილებენ დაკისრებულ ვალდებულებებს შესაბამისად.
- რადგანაც საქმიანობა ძირითადად ხორციელდება მაღალი უსაფრთხოების არეალში, ამ ტიპის ოთახებს მინიმუმ ერთი დაცვის სუბიექტი უნდა ყავდეს მიმაგრებული.
- საჭიროების შემთხვევაში უნდა შესრულდეს გადაუდებელი პროცედურების დაცვა და მისი შესაბამისი შესრულება წესების მიხედვით.

5.1.3 ძირითადი სახელმძღვანელოები

ორგანიზაციამ უნდა დაიქირაოს დაცვის თანამშრომელი, ან შესაბამისი პირი, რომელიც უზრუნველყოფს ფიზიკური უსაფრთხოების მოთხოვნების შესრულებას არსებული განაწესის გათვალისწინებით. აღნიშნული მოთხოვნები უნდა აკმაყოფილებდეს შემდეგ კრიტერიუმებს:

- დაცვის თანამშრომლის მოვალეობის შესრულებას პოზიციის მიხედვით.
- გარე და შიდა პერიმეტრის წვდომის კონტროლი
- ვიდეო დაკვირვების კამერების მონიტორინგი
- წვდომის ელექტრონული ბარათების ადმინისტრირება(შენახვა, გადაცემა და სხვა)
- საგანგაშო სიტუაციების მონიტორინგი და კონტროლი
- ფიზიკურ ინციდენტებზე რეაგირება
- გაუთვალისწინებელი მოვლენებზე რეაგირება
 - ბუნებრივი სტიქიები
 - ტერორიზმი

5.1.4 უსაფრთხოების ტრეინინგები

დაცვას უნდა უტარდებოდეს რეგულარული უსაფრთხოების ტრეინინგები და მათ გათვითცნობიერებული უნდა ქონდეთ სამსახურეობრივი მოვალეობები და პასუხისმგებლობა.

5.2 ვიზიტორები

ორგანიზაციაში ვიზიტორის(სტუმარი) შემოშვება უნდა ხდებოდეს წინასწარი რეგისტრაციის საფუძველზე, რომელშიც მითითებული უნდა იქნას მისი სახელი და ორგანიზაცია.

სტუმრებისათვის ძირითადად განკუთვნილია ოფისის არე, მაგრამ თუ ისინი ითხოვენ წვდომას მაღალი უსაფრთხოების არეში, თავდაპირველად აუცილებელია ნებართვის მოპოვება ორგანიზაციის უსაფრთხოების მენეჯერისგან.

ნებისმიერ შემთხვევაში ვიზიტორის წვდომა ორგანიზაციაში უნდა ხდებოდეს მისაღები არის გავლით და უნდა იყოს მუდმივად ესკორტირებული.

5.2.1 რეგისტრაციის პროცედურები

ორგანიზაცია ვალდებულია ყველა ვიზიტორისათვის შენობაში წვდომის დროს გაატაროს წინასწარ განსაზღვრული რეგისტრაციის პროცედურები. პროცედურები მოიცავს:

- წინასწარი რეგისტრაციის გადამოწმება
- პირადობის მოწმობის ან პასპორტის სამჯელზე პიროვნების დაგენა

ვენდორი ვალდებულია მოახდინოს ყველა ვიზიტორის ოფისში წვდომის აღრიცხვა ელექტრონულად ან სპეციალურ ფიზიკურ ფორმაში, რომელიც უნდა შეიცავდეს შემდეგ მონაცემებს:

- სტუმარის სახელი
- პირადი ნომერი
- კომპანია
- მიმღების სახელი
- ვიზიტის მიზანი
- მიღების უნიკალური ნომერი
- შესვლის და გასვლის დროები
- ხელმოწერა

აღნიშნული მონაცემები უნდა ინახებოდეს მინიმუმ 90დღის განმავლობაში.

5.2.2 ვიზიტორის იდენტიფიკაცია

დაცვა ვალდებულია ორგანიზაციაში შემვებამდე ვიზიტორს უნდა გააცნოს მინიმალური უსაფრთხოების მოთხოვნები და ინსტრუქტაჟი გაუწიოს ID ბეჯის გამოყენების შესახებ(ორგანიზაციაში ასეთის არსებობის შემთხვევაში). მაგალითად ID ბეჯი გააღებს კონკრეტულ კარებს და არეში შესვლამდე უნდა მოხდეს ID ბარათის მიღება სპეციალურ წამკითხველზე.

ორგანიზაციაში დაშვებულ ვიზიტორი მუდმივად უნდა ატარებდეს დაცვის მიერ მინიჭებულ იდენტიფიკატორს(ID ბეჯი, სტიკერი), რომელსაც უნდა ეწეროს ვიზიტორის სახელი და იდენტიფიკატორის ვალიდურობის დრო.

პირი, რომელიც უზრუნველყოფს სტუმრის ესკორტირებას, ვალდებულია ოფისის დატოვებისას ვიზიტორს დაატოვებინოს მისთვის გამოყოფილი ავტორიზაციის ID ბეჯი ან სტიკერი დაცვასთან.

5.2.3 სერვისის გარე პროვაიდერები

ამ ტიპის სტუმრებისათვის ორგანიზაციაში უნდა არსებობდეს სპეციალური დაშვების სია, სადაც გაწერილი იქნება მათი დაშვების ვადა და პირადი მონაცემები, ასევე მათთვის უკვე გამზადებული იქნება რეგისტრაციის იდენტიფიკატორები და მათ არ მოუწევთ ყოველ ვიზიტზე საწყისი სტანდარტული რეგისტრაციის პროცედურების გავლა.

აღნიშნულ დოკუმენტს უნდა ადასტურებდეს უსაფრთხოების მენეჯერი.

6. გარე პერიმეტრი

6.1 შენობის გარე სტრუქტურა

აუცილებელია აღმოფხვრილი იქნას არავტორიზებული წვდომა შენობის ისეთ არეებზე, სადაც განთავსებულია ტექნიკური მოწყობილობები, როგორებიცაა გაგრილების სისტემები, კვების გენერატორები და სხვა.

აღნიშნულ არეებამდე მისასვლელი კარები დაცული უნდა იყოს ელექტრული განგაშის მოყობილობებით, რომლებიც მიერთებული არიან უსაფრთხოების კონტროლის ოთახთან.

საჭიროებისამებრ ზემოთ ხსენებულ კარებზე დამონაწეხული განგაშის სისტემის გათიშვა უნდა იყოს შესაძლებელი. გათიშვის შემთხვევაში უნდა მოხდეს შემდეგი მონაცემების აღრიცხვა:

- თარიღი
- დრო
- პირი, რომელიც საჭიროებს დაშვებას
- დაშვების მიზეზი

6.2 შენობაში შესასვლელი და გასასვლელი წერტილები

ყველა არასაგანგაშო წერტილი უნდა:

- იყოს აღჭრევილი განგაშის მონიტორინგის სისტემით
- იყოს ფიზიკურად ჩაკეტილი ან ელექტრონულად კონტროლირებადი
- აღჭრევილი წვდომის დაშვების მექანიზმით. ბარათის წამკითხავი ან ბიომეტრია
- აღჭრევილი გისოსებით, რათა აღმოფხვრილი იქნას არავტორიზებული წვდომა

6.3 შენობის კედლები, ფანჯრები და კარები

შენობის ყველა გარე კედელი უნდა იყოს ქარხნულად დამზადებული, აგურის ბლოკისა ან ტოლფასი სიძლიერის მასალისგან, რათა შეძლოს არასანქცირებული შეღწევის აღკვეთა;

ასევე ანალოგიურად გარე ფანჯრები, კარები თუ ნებისმიერი ტიპის შესასვლელი უნდა იქნას აღჭრევილი არასანქცირებული შეღწევისგან დამცავი მექანიზმებით, როგორებიცაა, მაგალითად: გამძლე მინა, გისოსი, მინის ჩამსხვრევის დეტექტორი, მოძრაობისა დეტექტორი, ელექტრონული თუ მაგნიტური ჩამკეტი და სხვა.

6.4 შენობის პერიმეტრის უსაფრთხოება

ვენდორმა არ უნდა განათავსოს მოწყობილობები (მაგ., გადამზიდავები, ნაგვის კონტეინერი, ხელსაწყოები თუ სხვა) კედელთან, რომელიც იცავ შენობის გარე პერიმეტრს. ვენდორის შენობა განთავსებული უნდა იქნას ისეთ რაიონში, რომელსაც დროულად მოემსახურება საზოგადოებრივი სამართალდამცავი თუ ხანძარსაწინააღმდეგო სამსახურები.

ნაგებობა დაცული უნდა იქნას სიგნალიზაციის სისტემებით და სისტემა აღჭურვილი უნდა იქნას დამხმარე კვების სისტემებით, რათა დენის უკმარისობის/გათიშვის შემთხვევაში სისტემამ შეძლოს ოპერირება მინიმუმ 48 საათის გამწვანებაში.

სარეზერვო (ბექაპ) სისტემაზე გადასვლის შემთხვევაში, ყველა სისტემამ რეალურ დროში უნდა აცნობოს ვენდორს აღნიშნული ფაქტი.

ყველა გარე შემოსასვლი თუ გასასვლი, მათ შორის სატვირთო თუ ტექნიკური სამუშაოებისთვის განკუთვნილი, უნდა იქნას აღჭურვილი საჭვრეტელით, უსაფრთხოების ფანჯრით ან დახურული სატელევიზიო სისტემით (CCTV), რომელიც საშუალებას აძლევს უსაფრთხოების პერსონალს კონკრეტული გარე პერიმეტრის ვიზუალურად დათვალიერებისა, რათა არასანქცირებული წვდომის შემთხვევაში მოახდინონ ადექვატური რეაგირება.

რეკომენდირებულია გარე კარებზე დამონტაჟებული სიგნალიზაციის სისტემა შემოწმდეს სამ თვეში ერთხელ, რათა თავიდან აიცილოს ორგანიზაციამ შესაძლო ხარვეზები.

6.5 საავარიო გასასვლელები

ყველა საგანგებო გასასვლელზე უნდა იყოს დამონტაჟებული ლოკალური ხმოვანი სიგნალიზაციის სისტემა, რომელიც უნდა იმყოფებოდეს 24 საათიანი მონიტორინგის ქვეშ. აღნიშნულ გასასვლელებზე ასევე მითითებული უნდა იყოს წარწერა: „ საგანგებო

გასასვლელი კარი სიგნალიზაციით“. ასევე საგანგებო გასასვლელ კარებზე უნდა იქნას დამონტაჟებული ავტომატური საკეტები, რათა უზრუნველყოს მათი ავტომატურად ჩაკეტვა.

საგანგებო გასასვლელები უნდა იქნენ აღჭურვილნი კონტაქტური სიგნალიზაციის სისტემით. აღნიშნული გასასვლელები უნდა იქნან გამოყენებულნი მხოლოდ საგანგებო შემთხვევებში და არა რაიმე სხვა მიზნით.

სამუშაო საათებში, შიდა უსაფრთხოების კონტროლის ოთახმა ან მონიტორინგის სერვისის ცენტრის პერსონალმა უნდა მიიღოს განგაშის სიგნალი საგანგებო გასასვლელიდან;

არასამუშაო საათებში, საგანგებო გასასვლელის განგაშის სიგნალი უნდა მიეწოდოს და გამოძახებულ იქნას ადგილობრივი პოლიცია ან დაცვის თანამშრომელი, რომელიც პასუხისმგებელია რეაგირებაზე, ცენტრალური მონიტორინგის ან შიდა უსაფრთხოების სამსახურის დავალებით.

6.6 გარე განათება

გარე განათება უნდა ანათებდეს როგორც შენობის გარე პერიმეტრს, ასევე ყველა შესასვლელსა თუ გადაცემა-მიწოდების ადგილს და უნდა იძლეოდეს აღნიშნულ არეში მყოფ ინდივიდთა იდენტიფიცირების საშუალებას.

ვენდორმა ყოველ თვე უნდა შეამოწმოს გარე განათების ფუნქციონირება და ამ შემოწმების ჩანაწერი შეინახოს 24 თვის განმავლობაში.

6.7 სახურავის უსაფრთხოება

ხეები, სატელეფონო ბოძები, ღობეები და ა.შ., რომელნიც განთავსებულნი არიან შენობის ტერიტორიაზე და იძლევიან შენობაში სახურავიდან შესვლის საშუალებას აუცილებელია იქნან მოშორებულნი, გადატანილი ან დამატებითი გზებით დაცულნი, არანქცირებული წვდომის აღმოფხვრის მიზნით. შენობის სახურავის ამ ტიპის ყველა წერტილი უნდა იქნას ჩაკეტილი ან შიგნიდან კონტროლირებადი.

ყველა შეღწევის წერტილს უნდა გააჩნდეს მაგნიტური ან კონტაქტური სენსორები, რომლებიც უნდა ახდენდნენ შეღწევის მონიტორინგს;

ყველა ზედა განათება, სავენტრაციო და გაგრილების სისტემის მილები, რომლებიც აღწევენ შენობის პერიმეტრში, დაცულნი უნდა იქნან გისოსებით, არასანქცირებული შეღწევის თავიდან აცილების მიზნით.

6.8 გარე პერიმეტრის კონტროლის კამერები

გარე პერიმეტრის დახურული სატელევიზიო სისტემის კამერები ფოკუსირებული უნდა იყოს შენობის ყველა შესასვლელსა და გასასვლელზე, უნდა იჭერდეს მკაფიო სურათს ყველა პიროვნებისა, რომლებიც შემოდინან ან ტოვებენ შენობას. ასევე კამერები სამუშაო საათების განმავლობაში უნდა მონიტორინგდებოდეს უსაფრთხოების კონტროლის ოთახში.

7. ოფისის არე/მიმღები არე

შენობის მთავარი შესასვლელი ვიზიტორს უნდა მიუძღვებოდეს მისაღებ არეში, სადაც შეზღუდულია ფიზიკური კონტაქტი ვიზიტორსა და დაცვას/მიმღებ პირს შორის;

მისაღები არე უნდა იქნას აღჭურვილი გადაადგილების საკონტროლო მექანიზმებით (მაგ. „Mantrap” ან “Interlocking”).

მიმღები პირი ან დაცვის თანამშრომელი, რომლებიც პასუხისმგებელნი არიან ვიზიტორთა მიღება-გაცილებაზე, აუცილებელია ნებისმიერ დროს გააჩნდეთ მისაღები არეს თავისუფლად დათვალიერების საშუალება. შენობაში შეშვებამდე, ვიზიტორები აუცილებელია ვიზუალურად შემოწმდნენ მისაღებ არეში და დადასტურდეს მათი ვინაობა. ვენდორმა უნდა აწარმოოს ყველა იმ თანამშრომელთა სია, რომელთაც შეუძლიათ ვიზიტორების შენობაში შემოყვანა. მხოლოდ სიაში აღნიშნულ პირებს შეუძლიათ ვიზიტორების შემოყვანა.

ვიზიტორებს მხოლოდ მას შემდეგ მიეცემათ შენობაში შესვლის საშუალება, როდესაც მოხდება მათი იდენტიფიცირება და გადაეცემათ შესაბამისი საიდენტიფიკაციო

ბარათი(რეგისტრაციის დამადასტურებელი საბუთი), რომელსაც ისინი ატარებენ შენობაში გადაადგილების განმავლობაში;

ვიზიტორთა წვდომის დაშვების სისტემის ფუნქციონირებისათვის საჭირო ელექტრონული კონტროლის მექანიზმები განთავსებულ იქნას მიმღების სამუშაო მაგიდასთან ან უსაფრთხოების კონტროლის თახში. თუ გარე კარების ფუნქციონირებისთვის საჭირო ელექტრონული კონტროლის მექანიზმი განთავსებულია მიმღების სამუშაო მაგიდასთან, გამყოფი კედელი მიმღების არესა და მისაღებ ოთახს შორის უნდა იქნას აღჭურვილი უსაფრთხოების ფანჯრით - მაგ. ფანჯარა უნდა იყოს ტყვია გაუმტარი, გამჭირვალე მასალის, რომელსაც უნდა გააჩნდეს ჭრილი დაცვის თანამშრომლისთვის პატარა პაკეტებისა თუ დოკუმენტების გადასაცემად.

ორგანიზაციამ უნდა უზრუნველყოს ამ ზონაში მომუშავე თანამშრომლები ტელეფონით და საგანგაშო ღილაკით, რომელიც გააქტიურებს უხმო სიგნალიზაციას ცენტრალური მონიტორინგის სამსახურში ან პოლიციაში.

თუ მიმღების ზონა მოთავსებულია ან მოქმედებს, როგორც უსაფრთხოების კონტროლის ოთახი.

არასამუშაო საათებში უსაფრთხოების ყველა მექანიზმი (მათ შორის სიგნალიზაციის ჩართვა-გამორთვა) ელექტრონულად უნდა მონიტორინგდებოდეს შიდა უსაფრთხოების მონიტორინგის სისტემით ან კომპანიის კერძო ცენტრალური მონიტორინგის კომპანიით.

თანამშრომლებს შენობაში შესვლა უნდა შეეძლოთ მთავარი შესასვლელით ან მხოლოდ თანამშრომლებისთვის განკუთვნილი შესასვლელით. შენობის გარეთა შემოსასვლელი კარები პირდაპირ არ უნდა გადიოდეს მაღალი უსაფრთხოების ზონის შესასვლელთან (HSA).

8. მაღალი უსაფრთხოების არეალი

8.1 უსაფრთხოების კონტროლის ოთახი

ეს არის დახურული სატელევიზიო მონიტორინგის სისტემის (CCTV), არასანქცირებული წვდომის, სახანძრო და სიგნალიზაციის სისტემებით უზრუნველყოფისა და კონტროლის ძირითადი ოთახი.

ანუ ვენდორმა უნდა:

ყოველთვის უზრუნველყოს თანამშრომლის ყოფნა ოთახში, მაშინ როდესაც სამუშაოები მიმდინარეობს მაღალი უსაფრთხოების ზონაში (HSA);

უნდა განათავსოს უსაფრთხოების კონტროლის ოთახი მაღალი უსაფრთხოების ზონისგან განცალკევებით, რათა მიღწეულ იქნას მოვალეობრივი იზოლაცია და დამოუკიდებლობა დაცვასა და მაღალი უსაფრთხოების ზონის თანამშრომლებს შორის;

იმ შემთხვევაში, თუ უსაფრთხოების კონტროლის ოთახი მდებარეობს შენობის გარეთ, იგი აუცილებელია აშენებულ იქნას ბეტონის ბლოკით ან სხვა ტოლფასოვანი მასალით. კარებზე დაამონტაჟოს ბარათით დაშვების კონტროლის სისტემა, რომელსაც ჩართული ექნება „anti pass back“ ფუნქციონალი და დაკავშირებული იქნება კომპიუტერთან, რომელიც ჩაიწერს ყველა შესვლა-გამოსვლას.

ასევე უნდა დაამონტაჟოს კარებზე ავტომატური დაკეტვის მექანიზმი. თუ კარები ღიაა 30 წამის გამავლობაში ავტომატურად უნდა ჩაირთოს სიგნალიზაცია. დაშვების კონტროლის სისტემა უნდა იყოს დაპროგრამებული, რომლის მიხედვითაც თანამშრომელთა დაშვება ოთახში ხდება თანმიმდევრულად და უზრუნველყოფს მხოლოდ ავტორიზებულ პირთა დაშვებას;

უზრუნველყოს, რომ თითოეული ინდივიდუალის შესვლა და გამოსვლა ავსებს საიდენტიფიკაციო ბარათის შესვლის და გამოსვლის მთლიან ციკლს.

ასწავლოს დაცვის თანამშრომლებს უსაფრთხოების კონტროლის ოთახში საიდენტიფიკაციო ბარათის დაშვების კონტროლის სისტემისა და დახურული სატელევიზიო მონიტორინგის სისტემის (CCTV) ეფექტური გამოყენება. იგი უნდა დარწმუნდეს, რომ უსაფრთხოების დაცვის თანამშრომელი თვალს ადევნებს დახურული სატელევიზიო მონიტორინგის სისტემის (CCTV)-ის კადრებს რეალურ დროში.

აღიჭურვოს ოთახი ტყვიაგაუმტარი უსაფრთხოების ფანჯრით, რომელიც ხელს შეუწყობს გასაღებებისა და დოკუმენტების გაცვლას უსაფრთხოების თანამშრომლებსა და გარე ვიზიტორებს ან მაღალი უსაფრთხოების ზონის თანამშრომლებს შორის, ამ დროს მინიმუმადე არის შემცირებული არაავტორიზებულ თანამშრომელთან კონტაქტი და წვდომა;

ასევე უნდა აღჭურვოს ნებისმიერი სხვა გარე ფანჯარა ტყვიაგამძლე და სარკისებური შუბით, რათა აღმოფხვრილ იქნას შენობის გარედა.

8.2 უსაფრთხოების დაცვა და წვდომის პროცედურები

დაშვება მაღალი უსაფრთხოების ზონაში უნდა ეძლეოდეთ მხოლოდ ავტორიზებულ პირებს დაშვების კონტროლის სისტემის მეშვეობით, რომელიც მუშაობს ინდივიდთა თანმიმდევრულად დაშვების პრინციპით (person-by-person).

დაშვების კონტროლის სისტემები:

მუდმივად უნდა იქნას დაკავშირებული კომპიუტერთან, რომელიც ამონიტორინგებს და იწერს ყველა თანამშრომლისა თუ ვიზიტორის გადაადგილებას.

დაიცვას თანამშრომლები სპეკულაციისგან (piggybacking), უზრუნველყოს თანამშრომელთა თანმიმდევრობით შეშვება.

აღასრულოს ორმაგი თანდასწრება. თუ ერთ წუთზე მეტი ხნის განმავლობაში ოთახში იმყოფება ორზე ნაკლები პირი, მაშინ უნდა ჩაირთოს სიგნალიზაცია.

ვენდორმა უნდა დააპროგრამოს დაშვების კონტროლის სისტემა ისე, რომ მოხდეს მხოლოდ ავტორიზებულ პირთა შეშვება და ისიც მხოლოდ თანმიმდევრობით. დაშვების კონტროლის სისტემამ უნდა გააქტიუროს სიგნალიზაციის სისტემა ყოველთვის, როცა უკანასკნელი პირი დატოვებს მაღალი უსაფრთხოების ზონას. მაღალი უსაფრთხოების ზონა და ყველა განცალკევებული ოთახი ან ზონაში, უნდა იქნას აღჭურვილი მოძრაობის დეტექტორებით.

მოძრაობის დეტექტორმა უნდა ატეხოს განგაში მაშინ, როცა პროგრამული უზრუნველყოფის მნიშვნელობა იქნება 0-ის ტოლი (ანუ ოთახი წესით ცარიელია). ასევე სისტემამ უნდა ატეხოს განგაში მაშინ, როცა პროგრამული უზრუნველყოფის მნიშვნელობა 1-ის ტოლია (ანუ ოთახში ვინმე იმყოფება), მოძრაობის დეტექტორი ვერ მოახდეს მოძრაობის დაფიქსირებას. განგაში უნდა იყოს ლოკალური ხმოვანი სიგნალი. ამასთანავე, სამუშაო საათების დასრულების შემდეგ, სიგნალი უნდა მივიდეს კერძო უსაფრთხოების კონტროლის კომპანიასა ან პოლიციაში.

არავის ააქვს უფლება შეიტანოს პირადი ნივთები მაღალი უსაფრთხოების ზონაში (მაგ., სადილის კონტეინერები, რაიმე შეკვრა, ჩანთა) ან ნებისმიერი ელექტრონული მოწყობილობა მაგ. მობილური ტელეფონები, ფოტოკამერები და ა.შ).

8.3 ოთახები

განცალკევებული ოთახები მაღალი უსაფრთხოების ზონაში უნდა აკმაყოფილებდეს ყველა ზემოაღნიშნულ მოთხოვნებს, გარდა თანამშრომელთა თანმიმდევრობით დაშვების მოთხოვნისა (person -by-person).

მაღალი უსაფრთხოების ზონაში საპირფარეშო ოთახები არის აკრძალული, გარდა იმ შემთხვევისა, როდესაც საპირფარეშოების არსებობას სახელმწიფო კანონი მოითხოვს. თუ საპირფარეშოები გამოიყენება, მისასვლელი გზა უნდა კამერით მონიტორინგდებოდეს.

ამიტომ მაღალი უსაფრთხოების ზონის ფარგლებში შეიძლება არსებობდეს შემდეგი განცალკევებული ოთახები:

8.4 საცავი

საცავი წარმოადგენს მთავარ უსაფრთხო ზონას ვენდორის შეობაში.

საცავში უნდა ინახებოდეს:

- პერსონალის შესახებ პირადი ინფორმაცია;
- უსაფრთხოების კომპონენტები;
- გასანადგურებელი მასალა;
- ორგანიზაციის საბუთები, კონტრაქტები.

პროდუქტები, რომლებიც საჭიროებენ მიმწოდებლისთვის დაბრუნებას.

საცავი უნდა იყოს აშენებული რკინაბეტონის ნაგებობით (მინიმუმ 15 სმ ან 6 ინჩი) ან იმ მასალისგან, რომელიც იგივე ძალისა და გამძლეობის ტოლფასია.

შენობის გარეთა კედელი არ უნდა იქნეს გამოყენებული საცავის კედლად;

ფანჯრების გამოყენება არ არის დაშვებული;

საცავში შესვლა უნდა მოხდეს მხოლოდ საცავის კარისა ან გისოსების გავლით;

საცავის კედლებზე, იატაკსა და ჭერზე უნდა იქნას დამონტაჟებული საკმარისი რაოდენობის დაზიანების დეტექტორები;

საცავი დაცული უნდა იქნას რკინის კარით, რომელსაც გააჩნია ორმაგი საკეტი მექანიზმი (ფიზიკური ან ლოგიკური), რომელიც უზრუნველყოფს კარის გაღების ორმაგ

კონტროლს (კარის გაღება შეუძლებელი უნდა იყოს ერთი პიროვნების მიერ). საცავის კარის გაღება და დაკეცვა ყოველთვის უნდა მოხდეს ორი პიროვნების მიერ;

თუ საცავის კარი აუცილებელია იქნას ღია სამუშაო დღის განმავლობაში, მაშინ უნდა გამოყენებულ იქნას შიდა გისოსები. საცავის კარი ან შიდა გისოები ყოველთვის უნდა იყოს დაკეტილი, გარდა იმ შემთხვევისა, როცა თანამშრომელი მოითხოვს სარდაფში შესვლას რაიმეს შესანახად ან გამოსატანად. შიდა გისოსებზე ასევე დამონტაჟებული უნდა იყოს ორმაგი კონტროლის ფიზიკური ან ლოგიკური ჩამკეტი მექანიზმი.

საცავის კარი ან შიდა გისოსები აღჭურვილი უნდა იყოს ავტომატური დაკეტვის მექანიზმით და ავტომატურად უნდა ააქტიურებდეს ხმოვან სიგნალს ლოკალურად ან უსაფრთხოების კონტროლის ოთახში, თუ კარები ღია დარჩება 60 წამის განმავლობაში.

ყველა დაშვების ბარათის გარეშე წვდომა საცავში უნდა აღირიცხოს ჩანაწერებში. ჩანაწერები შესაძლებელია იყოს როგორც ფიზიკური, ასევე ელექტრონული;

საცავი უნდა იყოს ორგანიზებული ისე, რომ შესაძლებელი იყოს ნებისმიერი საქონლის ადგილმდებარეობის იდენტიფიცირება და დახურული სატელევიზიო მონიტორინგით (CCTV) თვალყურის დევნება არის სავალდებულო

8.5 შიდა უსაფრთხოება

იმისათვის, რომ მოხდეს უსაფრთხოების ოთახში და მიმდებარე ტერიტორიაზე მომუშავე პერსონალის გაფრთხილება, როდესაც კარები ან გისოსები მკაცრად დაცულ ადგილას არის ღიად დატოვებული 30 წამზე მეტი ხნის განმავლობაში, ადგილობრივი სიგნალიზაცია და/ან მოციმციმე სიგნალიზაციის ნათურები უნდა ამოქმედდეს, თუ სხვა რამ არ არის განსაზღვრული ამ დოკუმენტში.

სიგნალიზაციის სისტემა აღჭურვილი უნდა იქნას დამატებითი ძალის მიმცემი ან დამხმარე კვების სისტემებით, რათა დენის უკმარისობის/გათიშვის შემთხვევაში სისტემამ შეძლოს ოპერირება მინიმუმ 48 საათის განმავლობაში;

სარეზერვო (ბექაპ) სისტემაზე გადასვლის შემთხვევაში, ყველა სისტემამ რეალურ დროში უნდა აცნობოს ვენდორს აღნიშნული ფაქტი;

სიგნალიზაციის აქტივაცია და დეაქტივაცია უნდ შემოწმდეს და დადასტურდეს ელექტრონული მექანიზმის, დაცვის, კომპანიის კერძო უსაფრთხოების სამსახურის ან პოლიციის მეშვეობით, რათა უზრუნველყოფილ იქნას, რომ წინასწარ დაგეგმილი სიგნალიზაციის დროის მახასიათებლები ძალაშია. სიგნალიზაციის გამორთვის დროს უნდა წარმოიქმნას ჩუმი განგაში (არაავტორიზებული ქმედებების თავიდან აცილების მიზნით).

- უნდა დადგინდეს კონკრეტული პროცედურა, რათა უზრუნველყოფილ იქნეს სწრაფი რეაგირება, ისეთი შემთხვევისათვის, თუ სიგნალიზაცია არ ამოქმედდა წინასწარ დაგეგმილი დროის პარამეტრების შესაბამისად;

- სიგნალიზაციის ჩართვისა და გამორთვის კოდები ცნობილი უდა იყოს მხოლოდ ავტორიზებული თანამშრომლისათვის;

- დაცვამ და თანამშრომლებმა უნდა დაიცვან აღნიშნული პროცედურა სიგნალიზაციის ამოქმედების შემთხვევაში. ეს პროცედურები ნათლად უნდა იყოს აღწერილი შიდა უსაფრთხოების პროცედურებში;

წვდომის კონტაქტები და მოძრაობის დეტექტორები უნდა ამოქმედებულ იქნან იმ ზონებში, სადაც თანამშრომლები არ იმყოფებიან (მაგ., საცავი, წარმოების ზონა, მიღება-ჩაბარების ზონა).

8.6 განგაშის სისტემები და ღილაკები

ადგილმდებარეობა

განგაშის ღილაკები განთავსებული უნდა იყოს შემდეგ ადგილებში:

- ა) ვიზიტორთა მისაღებში, უსაფრთხოების კონტროლის ოთახში ან ორივეგან ერთდროულად;
- ბ) საცავში;
- გ) მიღება-ჩაბარების ზონაში;

დ) თანამშრომელთა შემოსასვლელში.

გააქტიურება

ა) განგაშის ღილაკის გააქტიურებისას, გაფრთხილების ან განგაშის სიგნალი უნდა გაიგზავნოს უსაფრთხოების კონტროლის ოთახში, ცენტრალური დისტანციური მონიტორინგის პუნქტში, ან პოლიციაში. რეაგირება (მაგ., განგაშის გადამოწმება) უნდა მოხდეს ორი წუთის განმავლობაში.

ბ) ყველა დეტალი, რაც დაკავშირებულია განგაშის გააქტიურებასა და რეაგირებაზე ცენტრალური დისტანციური მონიტორინგის პუნქტისა თუ პოლიციის მხრიდან, უნდა იწერებოდეს სპეციალურად განკუთვნილ ჟურნალში, რომელშიც უნდა იწერებოდეს შემდეგი სახის ინფორმაცია:

- განგაშის ღილაკის გააქტიურების დრო და თარიღი.
- ცენტრალური დისტანციური მონიტორინგის პუნქტიდან რეაგირების დრო.
- პოლიციიდან ან სხვა დახმარების გზებიდან რეაგირების/ადგილზე გამოცხადების დრო.
- ყველა განხორციელებული ქმედებების ქრონოლოგია, მათ შორის პირთა ვინაობები, რომლებიც უშუალოდ იყვნენ ჩართულნი;
- სიგნალიზაციის გააქტიურების მიზეზი.

შესაბამისად ყველა განგაშის ღილაკი უნდა გაიტესტოს კვარტალურად და შედეგები აღირიცხოს დოკუმენტში.

8.7 საკეტები და გასაღებები

ტერმინი „გასაღები“, ეხება ყველა ფიზიკურ გასაღებს ან გასაღებთა კომბინაციას, რომელიც იძლევა შეზღუდულ ზონაში წვდომის საშუალებას, მათ შორის მაღალი უსაფრთხოების ზონაში განთავსებულ ნებისმიერ არეში.

თანამშრომელი, რომელიც მიიღებს გასაღებს ხელს აწერს სპეციალურ ფორმას, რომლითაც ადასტურებს, რომ მან მიიღო გასაღები და იგი არ ჩავარდება არავტორიზებული პირის ხელში.

ყველა ჯერ არ გაცემული გასაღები, მთავარი გასაღებები და გასაღების დუბლიკატები უნდა ინახებოდეს ორმაგი კონტროლის ქვეშ სეიფში ან უსაფრთხო კაბინეტში და გასაღებებზე პასუხისმგებელ პირთა ცვლილება და მათთვის გასაღებების გადაცემა უნდა აღირიცხოს სპეციალურად განკუთვნილ გასაღებების ჟურნალში.

გასაღებების მართვა უნდა სრულდებოდეს განცალკევებულ ოთახში, რომელიც არის მაღალი უსაფრთხოების პერსონალიზაციის ზონაში და შიდა დახურული სატელევიზიო მონიტორინგის (CCTV) კამერები უნდა დამონტაჟდეს ისე, რომ აკონტროლებდეს შესვლასა და შიდა მოქმედებას აღნიშნულ ოთახში. კამერას არ უნდა გააჩნდეს გადიდების ან სკანირების ფუნქციონალი და უნდა იქნას მიმართული ისეთ პოზიციაზე, რომ ახორციელოს თვალყურის დევნება კლავიშებსა თუ მონიტორის ეკრანზე.

და ბოლოს ნებისმიერი საკეტის კომბინაცია, სადაც კომბინაციის მფლობელს აქვს წვდომა უნდა შეიცვალოს, მაშინ როცა კომბინაციის მფლობელი წაიშლება ავტორიზებული მფლობელების სიიდან.

8.8 შიდა პერიმეტრის კონტროლის კამერები

ყველა კამერა (CCTV) უნდა გაიტესტოს ყოველ თვე და შემოწმდეს გამოსახულების ხარისხი. ვენდორმა უნდა შეინახოს ამ ტესტირების ჩანაწერები ორი წლის განმავლობაში;

კამერების უნებლიე ან თვითნებური გათიშვის შემთხვევაში, ვიდეოჩანაწერის დაკარგვა უნდა აისახოს მონიტორებზე, რომელიც მდებარეობს უსაფრთხოების კონტროლის ოთახში და თან დაერთოს ხმოვანი განგაშის სიგნალი;

როგორც ციფრული ჩანაწერები, ასევე დაშვების კონტროლის სისტემები უნდა იყოს სინქრონიზირებული რეალურ დროში. სისტემების სინქრონიზაცია უნდა იყოს ერთმანეთისაგან ორი წამის შუალედით;

ჩაწერის სისტემას უნდა შეემდოს ნებისმიერი ჩანაწერის ზედიზედ გამეორება, ისე, რომ არ შეწყდეს ჩაწერის პროცესი;

ე) სასერვერო და პინების ოთახის კამერებს არ უნდა ჰქონდეთ (ან უნდა გამოირთოს) გადიდებისა და სკანირების ფუნქციონალი.

მონიტორი, კამერა და ციფრული ჩამწერი მოწყობილობის მოთხოვნები

თითოეული მონიტორი, კამერა და ციფრული ჩამწერი უნდა მუშაობდეს გამართულად და მონიტორზე უნდა აჩვენებდეს ნათელ გამოსახულებას, არ უნდა იყოს ფოკუსი არეული, ბუნდოვანი ან ზედმეტად ჩაბნელებული. მოწყობილობამ უნდა ჩაიწეროს მინიმუმ ოთხი კადრი წამში;

კამერები უნდა უწყვეტად იწერდეს და ამონიტორებდეს ყველა მოქმედებას, მათ შორის უნდა შეეძლოს მოქმედების გადაღება სიბნელის დროს ინფრაწითელი სხივის ან ავტომატური პროექტორების საშუალებით;

დახურული სატელევიზიო სისტემის მონიტორები და ციფრული ჩამწერები მოთავსებულნი უნდა იყვნენ ისეთ ადგილებში, სადაც დაშვება არის შეზღუდული მხოლოდ ავტორიზებულ პირთათვის;

CCTV კამერები ყოველთვის დაკავშირებული უნდა იყვნენ:

- კონტროლის ოთახში მდებარე მონიტორთან;
- სიგნალიზაციის სისტემასთან, CCTV კამერების გათიშვის აღმოსაჩენად;
- აქტიური გამოსახულების ჩამწერ მოწყობილობასთან.

თითოეული კამერის ხედვის არეალი უნდა მოიცავდეს ყველა მოქმედებას, რაც აუცილებელია სათანადო უსაფრთხოების ზომების მისაღებას;

ჩაწერისას უნდა დაფიქსირდეს სათანადო გამოსახულებები, რათა მოხდეს პიროვნების იდენტიფიკაცია (მაგ., თავისა და მხრების ხედვა) და ასევე მის მიერ განხორციელებული ქმედებები;

თითოეული შიდა CCTV კამერა და ჩამწერი სისტემა აღჭურვილი უნდა იქნას ავტომატური ჩაწერის შესაძლებლობით, განგაშის შემთხვევაში.

ვიდეოჩანაწერების შენახვა

CCTV კამერების ჩანაწერები უნდა ინახებოდეს სულ მცირე 90 დღის განმავლობაში და ყოველდღიურად უნდა ხდებოდეს მათი დაბეჭადვა;

სარეზერვო ჩანაწერი უნდა ინახებოდეს შენობაში განცალკევებულ, უსაფრთხო ადგილას და უზრუნველყოფილ უნდა იქნას მოვალეობების გადანაწილება სისტემის მომხმარებლებსა და ადმინისტრატორებს შორის.

8.9 უსაფრთხოების მოწყობილობების ინსპექტირება

დავიწყეთ იქიდან, რომ აუცილებელია და მკაცრად რეკომენდირებულია ნახევარწლიანი გამოკვლევების ჩატარება ყველა უსაფრთხოების მოწყობილობისათვის, რაც დანერგილია ორგანიზაციაში, როგორებიცაა მინიმუმ:

- სიგნალიზაციის სისტემა;
- დაშვების კონტროლის სისტემა;
- ფანჯრებისა და კარების კონტაქტები;
- მინის მსხვრევის დეტექტორები;
- საგანგებო კარების სიგნალიზაცია;
- პასიური ინფრაწითელი დეტექტორები;
- მიკროტალღური სენსორები;
- მდუმარე განგაშის ღილაკები;
- CCTV მონიტორები;
- CCTV ჩამწერები.

გამოკვლევები უნდა განახორციელოს გარე ორგანიზაციამ, რომელიც კვალიფიციურია ამგვარი ფუნქციების შესრულებაში და გამოკვლევის რეპორტის ასლი უნდა ინახებოდეს მინიმუმ 18 თვის განმავლობაში.

კვების ელემენტის შემოწმება

კვების ელემენტები, რომელიც გამოიყენება ლოკალურ სიგნალიზაციაზე უნდა შემოწმდეს სულ მცირე ყოველ თვე და გამოიცვალოს ყოველწლიურად (ან მიმწოდებლის მიერ წარმოებული ტექნიკური მახასიათებლების შესაბამისად, თუ შემოწმება უფრო ხშირია);

ამ შემოწმების მტკიცებულებები (ჩანაწერები) უნდა ინახებოდეს მინიმუმ 18 თვის განმავლობაში.

8.10 აპარატურის განლაგება და დაცვა

ორგანიზაციაში აპარატურა უნდა მოთავსდეს და დაცული იქნას ისე, რომ შემცირდეს გარე ფაქტორებით გამოწვეული საფრთხე და არავტორიზებული წვდომის შესაძლებლობა. აპარატურის დასაცავად გასათვალისწინებელია შემდეგი პრინციპები:

ა) აპარატურა ისე უნდა დაინსტალირდეს, რომ სამუშაო ზონაში შემცირდეს არავტორიზებული წვდომა;

ბ) ინფორმაციის დამუშავების საშუალებები, რომლებსაც შეხება აქვთ მნიშვნელოვან მონაცემებთან, ისე უნდა განლაგდეს და მათი დანახვის კუთხე ისე შეიზღუდოს, რომ შემცირდეს არავტორიზებული პირების მიერ ინფორმაციაზე წვდომა, ასევე უნდა მოხდეს შენახვის საშუალებების დაცვა;

გ) აპარატურა, რომელიც განსაკუთრებულ დაცვას მოითხოვს, იზოლირებული უნდა იყოს, რათა შემცირდეს არსებული რისკის საერთო დონე;

დ) უნდა დაწესდეს შესაბამისი კონტროლი, რათა შემცირდეს პოტენციური ფიზიკური საფრთხის რისკი, მაგ.: ქურდობა, ხანძარი, აფეთქება, წყალი (წყლის მარაგის შეფერხება), კვამლი, მტვერი, ვიბრაცია, ქიმიური ეფექტი, ელექტროენერგიის მიწოდების შეფერხება, ელექტრომაგნიტური რადიაცია და ვანდალიზმი;

ე) უნდა დადგინდეს ინფორმაციის დამუშავების საშუალებების სიახლოვეს კვებისა და მოწევის წესები;

ვ) უნდა განხორციელდეს ტემპერატურის, ტენიანობის მონიტორინგი;

ზ) ყველა შენობაზე უნდა დამონტაჟდეს მეხამრიდი და მეხამრიდის ფილტრები უნდა მოერგოს ყველა შემომავალ ენერგო და კომუნიკაციის ხაზებს;

თ) ინდუსტრიულ გარემოში აპარატურისთვის გათვალისწინებული უნდა იქნას სპეციალური დაცვის მეთოდების გამოყენება, როგორიცაა მემბრანიანი კლავიატურა და ა.შ.

ი) აპარატურა, რომელიც მნიშვნელოვან ინფორმაციას ამუშავებს, დაცული უნდა იყოს იმგვარად, რომ შემცირდეს გამოსხივების გამო ინფორმაციის გაჟონვის რისკი.

დასკვნა

ფიზიკური უსაფრთხოების რისკების სათანადოდ შეუფასებულობის და შესაბამისი პრევენციული კონტროლების არ გატარების შემთხვევაში, ხდება ორგანიზაციაში არსებული ფასეული ინფორმაციის უსაფრთხოების დარღვევა და თავს იჩენს ინფორმაციის გაჟონვა, რასაც ორგანიზაციები სავალალო შედეგებამდე მიჰყავს. გამოუსწორებადი შედეგებში იგულისხმება: უზარმაზარი ფინანსური დანაკარგები, საკანონმდებლო დარღვევები, რეპუტაციის შელახვა და სხვა.

ფიზიკური უსაფრთხოების რისკების მართვის პროცესს ერთ-ერთი ყველაზე სასიცოცხლო მნიშვნელობა გააჩნია ნებისმიერი ორგანიზაციისთვის, რადგან ამ კომპონენტის გარეშე წარმოუდგენელია სამომავლო მისიისა თუ გეგმების სათანადოდ ან საერთოდ შესრულება.

გამოყენებული ლიტერატურა

1. PCI_Card_Production_Physical_Security_Requirements / Version 1.0, Mey 2013
2. DEA27002 / Version 1.0.1, 2011
3. Managing information security Risk / national Institute of standarts and Technology, Publication 800-39 , March 2011
4. CISSP-Certified-Information-Systems-Security-Professional-Study-Guide / James Michael Stewart Version 4.0, May 2014