დანართი

სსიპ - განათლების მართვის საინფორმაციო სისტემის მიერ ვიდეომონიტორინგის განხორციელების წესი

მუხლი 1. რეგულირების სფერო

1. სსიპ - განათლების მართვის საინფორმაციო სისტემის მიერ ვიდეომონიტორინგის განხორციელების წესი (შემდგომ - წესი) შემუშავებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის, სსიპ - განათლების მართვის საინფორმაციო სისტემის (შემდგომ - მართვის სისტემა) საქმიანობის მარეგულირებელი შესაბამისი ნორმატიული აქტებისა და საჯარო დაწესებულებების მიერ ვიდეომონიტორინგის განხორციელებასთან დაკავშირებით პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შემუშავებული რეკომენდაციების საფუძველზე და განსაზღვრავს მართვის სისტემის მიერ ვიდეომონიტორინგის განხორციელების მიზანს, მოცულობას, ხანგრძლივობას, ვიდეოჩანაწერის შენახვის ვადას, ვიდეოჩანაწერზე წვდომის, მისი შენახვისა და განადგურების წესსა და პირობებს და მონაცემთა სუბიექტის დაცვის მექანიზმებს.

მუხლი 2. წესის მიზანი

1. ამ წესის მიზანია მართვის სისტემის მიერ ვიდეომონიტორინგის კანონიერად განხორციელების უზრუნველყოფა, ვიდეომონიტორინგის განხორციელების პროცესში ჩართულ პირთა უფლება-მოვალეობებისა და მონაცემთა სუბიექტის დაცვის მექანიზმების განსაზღვრა.

მუხლი 3. ტერმინთა განმარტება

1. ამ წესში გამოყენებულ ტერმინებს აქვს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრული მნიშვნელობა.

მუხლი 4. ვიდეომონიტორინგის განხორციელების მიზანი

ვიდეომონიტორინგის განხორციელების მიზანია:

ა) მართვის სისტემის შენობასა და მიმდებარე ტერიტორიაზე უსაფრთხოების დაცვა;

ბ) მართვის სისტემისა და მართვის სისტემის თანამშრომელთა საკუთრების/უსაფრთხოების დაცვა;

გ) საზოგადოებრივი უსაფრთხოების, მართლწესრიგის დაცვის, მათ შორის, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების უზრუნველყოფა, დაწესებულებაში არსებულ საინფორმაციო სისტემებზე არამართლზომიერი წვდომის პრევენცია არაავტორიზებული პირების მიერ.

მუხლი 5. ვიდეომონიტორინგის განხორციელების ხანგრძლივობა და ფარგლები

1. მართვის სისტემა ვიდეომონიტორინგს ახორციელებს შენობის დერეფნებსა და მიმდებარე გარე პერიმეტრზე, მათ შორის, შენობის სახურავზე, 24 საათიან რეჟიმში, აუდიოჩანაწერის გარეშე, შემდეგ მისამართზე - ქალაქი თბილისი, გ. ფანჯიკიძის ქ. N1ა.

2. მართვის სისტემა ვიდეომონიტორინგს ახორციელებს, მის სარგებლობაში არსებულ სასერვეროზე, ასევე, სასერვეროს გაგრილების სისტემებისა და გენერატორების

ტერიტორიაზე, 24 საათიან რეჟიმში, აუდიოჩანაწერის გარეშე, შემდეგ მისამართზე - ქალაქი თბილისი, მერაბ ალექსიძის II შესახვევი N2.

3. ამ მუხლის პირველი პუნქტით გათვალისწინებულ მისამართზე ვიდეომონიტორინგის გეოგრაფიული არეალის ფარგლებში, შიდა და გარე პერიმეტრზე, განთავსებულია სულ 23 ვიდეოკამერა, რომელთაგან:

ა) გარე პერიმეტრზე განთავსებულია 12 ვიდეოკამერა, მათგან:

ა.ა) 9 ვიდეოკამერა მიმართულია შენობის გარშემო ტერიტორიაზე;

ა.ბ) 2 ვიდეოკამერა მიმართულია შენობის სახურავზე;

ა.გ) 1 ვიდეოკამერა მიმართულია შენობის აივანზე.

ბ) შიდა პერიმეტრზე განთავსებულია 11 ვიდეოკამერა, მათგან:

ბ.ა) 1 ვიდეოკამერა მიმართულია შენობის შემოსასვლელზე;

ბ.ბ) 5 ვიდეოკამერა მიმართულია შენობის პირველი სართულის დერეფნებზე;

ბ.გ) 5 ვიდეოკამერა მიმართულია შენობის მე-2 სართულის დერეფნებზე.

4. ამ მუხლის მე-2 პუნქტით გათვალისწინებულ მისამართზე ვიდეომონიტორინგის გეოგრაფიული არეალის ფარგლებში, შიდა და გარე პერიმეტრზე, განთავსებულია სულ 5 ვიდეოკამერა, რომელთაგან:

ა) 1 ვიდეოკამერა მიმართულია სასერვეროზე;

ბ) თითო ვიდეოკამერა მიმართულია სასერვეროს გაგრილების სისტემებსა და გენერატორებზე;

გ) თითო ვიდეოკამერა მიმართულია სასერვეროს გაგრილების სისტემებსა და გენერატორებზე გარედან;

5. მართვის სისტემის მიერ განხორციელებულ ვიდეომონიტორინგის არეალში ექცევიან მართვის სისტემის თანამშრომლები, მართვის სისტემაში მოსული სტუმრები და მიმდებარე გარე პერიმეტრზე მყოფი სხვა პირები.

6. მართვის სისტემის მიერ დასაქმებულთა სამუშაო ადგილზე (სამუშაო ოთახი) არ ხორციელდება ვიდეომონიტორინგი, გარდა იმ დასაქმებულთა სამუშაო ადგილისა, რომელთა სამუშაო ადგილიც წარმოადგენს შენობის დერეფანს და სამუშაო ოთახი არ არის დერეფნისგან გამოყოფილი ადგილი.

7. ამ მუხლის მე-4 პუნქტით განსაზღვრულ შემთხვევაში, მართვის სისტემის ფინანსური და მატერიალური რესურსების სამსახური უზრუნველყოფს დასაქმებულთა წერილობითი ფორმით ინფორმირებას, ვიდეომონიტორინგის მიმდინარეობისა და მათი უფლებების შესახებ.

8. ვიდეომონიტორინგი არ ხორციელდება გამოსაცვლელ ოთახებში, ჰიგიენისთვის განკუთვნილ ადგილებსა და შენობაში მდებარე სამუშაო ოფისებში, ასევე ისეთ სივრცეში, სადაც სუბიექტს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს ან/და ვიდეომონიტორინგის განხორციელება საყოველთაოდ აღიარებულ ზნეობრივ ნორმებს ეწინააღმდეგება.

მუხლი 6. ვიდეომონიტორინგის შესახებ გაფრთხილება

მართვის სისტემის მიერ ვიდეომონიტორინგის განხორციელების ადგილებში, თვალსაჩინო ადგილას განთავსებულია გამაფრთხილებელი ნიშანი, რომელიც მოიცავს ინფორმაციას ვიდეომონიტორინგის მიმდინარეობის შესახებ და მასზე დატანილია მონაცემთა დამუშავებაზე პასუხისმგებელი პირის სახელწოდება და საკონტაქტო მონაცემი.

მუხლი 7. ვიდეოჩანაწერის შენახვის ვადა

1. მართვის სისტემის მიერ განსაზღვრული ვიდეომონიტორინგის განხორციელების მიზნების გათვალისწინებით, მართვის სისტემის მიერ მოპოვებული ვიდეოჩანაწერები ინახება 30 (ოცდაათი) კალენდარული დღის მანძილზე, ჩამწერ მოწყობილობებში, მყარ დისკზე.

2. ვიდეოჩანაწერების შენახვის ვადის გასვლის შემდგომ, ჩამწერ მოწყობილობებში არსებული ჩანაწერები ავტომატურად იშლება, აღდგენის შესაძლებლობის გარეშე.

მუხლი 8. მონაცემთა უსაფრთხოება და მათზე წვდომა

1. მართვის სისტემის მიერ უზრუნველყოფილია ვიდეომონიტორინგის სისტემის ფიზიკური უსაფრთხოება და მიღებულია ჩანაწერების უსაფრთხოების დაცვისთვის აუცილებელი ორგანიზაციულ-ტექნიკური ზომები და ვიდეოჩანაწერები ინახება კონფიდენციალურობის, მთლიანობის, ხელმისაწვდომობის პრინციპების დაცვით.

2. ვიდეოსათვალთვალო სისტემაში (მათ შორის, ჩამწერ მოწყობილობებში) დაცულ ჩანაწერებზე, პროგრამული უზრუნველყოფის საშუალებით, წვდომის უფლებამოსილება ენიჭება მართვის სისტემის კომპიუტერული ტექნიკის მხარდაჭერის სპეციალისტსა და დაცვის თანამშრომლებს.

3. ამ წესის მე-5 მუხლის 1-ლი პუნქტით განსაზღვრულ მისამართზე, ვიდეომონიტორინგის რეალურ რეჟიმში დაკვირვება ხორციელდება მართვის სისტემის დაცვის თანამშრომლების მიერ.

4. იმ შემთხვევაში, თუ მართვის სისტემის რომელიმე სტრუქტურულ ერთეულს, სამსახურებრივი საქმიანობის შესრულებისათვის ესაჭიროება ვიდეოჩანაწერების გადამოწმება, ასეთი სტრუქტურული ერთეულის, დოკუმენტბრუნვის ელექტრონული სისტემის (Eflow) მეშვეობით მიმართავს, მართვის სისტემის უფროსს და წარუდგენს ინფორმაციას ვიდეოჩანაწერის თარიღისა და მოთხოვნის საფუძვლის თაობაზე შესაბამისი დასაბუთებით. იმ შემთხვევაში, თუ მართვის სისტემის უფროსი მოთხოვნის საფუძვლის, შესაბამისი დასაბუთების და ვიდეოჩანაწერის შინაარსის გათვალისწინებით მიზანშეწონილად მიიჩნევს ვიდეოჩანაწერის მომთხოვნი სტრუქტურული ერთეულისათვის გადამოწმების შესაძლებლობის მიცემას, შესაბამისი რეზოლუციით გასცემს თანხმობას და ავალებს შესაბამის პასუხისმგებელ თანამშრომელს, უზრუნველყოს მომთხოვნი სტრუქტურული ერთეულის წარმომადგენელთან ერთად, ვიდეო სამეთვალყურეო სისტემაში ვიდეოჩანაწერების გადამოწმება მითითებულ ვადაში.

5. ვიდეოჩანაწერის ასლის მესამე პირისათვის გადაცემა მართვის სისტემის მიერ უნდა განხორციელდეს მხოლოდ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით მკაცრად განსაზღვრულ შემთხვევებში. ვიდეოჩანაწერის ასლი მესამე პირს უნდა გადაეცეს მხოლოდ შესაბამისი კანონის მიზნისა და საფუძვლის არსებობის შემთხვევაში, მონაცემთა დამუშავებისათვის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი პრინციპების დაცვით.

6. ვიდეოჩანაწერის ასლის გამცემისა და ჩანაწერის ასლის მიმღების მიერ მიღებული უნდა იქნას ყველა აუცილებელი ზომა, მონაცემების უკანონო დამუშავების თავიდან ასაცილებლად.

7. ჩანაწერის ასლის გამცემი და ჩანაწერის ასლის მიმღები პირები ვალდებულნი არიან მოპოვებული მონაცემები დაამუშაონ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული მონაცემთა დამუშავების პრინციპების დაცვით.

8. მართვის სისტემის მიერ მიღებულია ზომები ინტერნეტიდან და კომპიუტერული ქსელიდან უკანონო შეღწევის თავიდან აცილების მიზნით, მიღებულია ტექნოლოგიურ-ორგანიზაციული ზომები, მათ შორის, რთული პაროლების, ორმაგი ავტორიზაციის, აღრიცხვის (ლოგირების) სისტემების, ამ სისტემების რეგულარული დატესტვისა და სხვა ტექნოლოგიურ-ორგანიზაციული მექანიზმების გამოყენებით.
9. მართვის სისტემის მიერ პერიოდულად მოწმდება სისტემაზე წვდომის შემთხვევები. არასანქცირებული წვდომის გამოვლენის შემთხვევაში, ხორციელდება შესაბამისი რეაგირება და გამომვლენი პირი ვალდებულია იმოქმედოს მართვის სისტემაში დადგენილი ინციდენტების მართვის პროცედურის შესაბამისად.
10. მართვის სისტემაში არსებული წვდომების და უფლებების გადამოწმების პროცედურის შესაბამისად ხორციელდება სისტემაში გაწერილი წვდომები და უფლებების პერიოდული გადამოწმება.
11. მართვის სისტემის თანამშრომლები ინფორმირებულნი არიან ვიდეომონიტორინგის გზით მოპოვებულ პერსონალურ მონაცემთა დაცვის მნიშვნელობის შესახებ და მათ მიერ პერსონალურ მონაცემთა დაცვის მიზნით შემუშავებული ნორმების დარღვევა წარმოადგენს დისციპლინური პასუხისმგებლობის დაწყების საფუძველს.
12. ვიდეოჩანაწერებზე, ამ წესის დარღვევით ან/და არასამსახურებრივი მიზნით წვდომის ფაქტის გამოვლენის და პრევენციის მიზნით, მართვის სისტემის კომპიუტერული სისტემების, ქსელებისა და კომუნიკაციის სამსახური უზრუნველყოფს ჩანაწერების მიმართ განხორციელებული ყველა მოქმედების აღრიცხვას, კერძოდ - თითოეული მოქმედების (მათ შორის, წვდომის), მოქმედების დროის და მოქმედების განმახორციელებელი მომხმარებლის იდენტიფიცირებას და შენახვას (ე.წ. ლოგირება). ასეთი ჩანაწერები ინახება არანაკლებ 6 (ექვსი) თვის ვადით.

მუხლი 9. მონაცემთა სუბიექტის უფლებები

1. მართვის სისტემა უზრუნველყოფს მონაცემთა სუბიექტის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის III თავით გათვალისწინებული უფლებების დაცვას.
2. მართვის სისტემა მონაცემთა სუბიექტის წერილობითი მოთხოვნის საფუძველზე, უზრუნველყოფს მონაცემთა სუბიექტის შემდეგი უფლებების რეალიზაციას:
ა) ვიდეოჩანაწერის ასლის მიღების უფლება;
ბ) ვიდეოჩანაწერის წაშლის და დაბლოკვის მოთხოვნის უფლება;
გ) ვიდეომონიტორინგის განმახორციელებელი პირის, ვიდეომონიტორინგის განხორციელების მიზნისა და სამართლებრივი საფუძვლის, მონაცემთა შენახვის ვადის, პერსონალურ მონაცემთა დაცვის ოფიცრის ვინაობისა და საკონტაქტო ინფორმაციის შესახებ ინფორმაციის მიღების უფლება;
დ) ვიდეოჩანაწერის სხვისთვის გადაცემის საფუძვლისა და მიზნის შესახებ ინფორმაციის მიღების უფლება.
3. ამ მუხლის მე-2 პუნქტით გათვალისწინებული უფლებების რეალიზაციის მიზნით, მონაცემთა სუბიექტი წერილობითი ფორმით - განცხადებით მიმართავს მართვის სისტემის უფროსს, ვიდეოჩანაწერის თარიღის მითითებითა და მოთხოვნის საფუძვლის თაობაზე შესაბამისი დასაბუთებით.
4. მართვის სისტემის უფროსი ამ მუხლის მე-3 პუნქტით გათვალისწინებულ განცხადებას, იმავე დღეს, უგზავნის პერსონალურ მონაცემთა დაცვის ოფიცერს, რომელიც გონივრულ ვადაში განიხილავს მოთხოვნას და იმ შემთხვევაში, თუ პერსონალურ მონაცემთა დაცვის

ოფიცერი მოთხოვნის საფუძვლის, შესაბამისი დასაბუთების და აუდიოჩანაწერის შინაარსის გათვალისწინებით, მიზანშეწონილად მიიჩნევს მონაცემთა სუბიექტის მოთხოვნის დაკმაყოფილებას, მოთხოვნის შინაარსიდან გამომდინარე, წერილობით ავალებს შესაბამის პასუხისმგებელ თანამშრომელს, უზრუნველყოს მონაცემთა სუბიექტის განცხადებაში მითითებული მოთხოვნის დაკმაყოფილება განსაზღვრულ ვადაში, რომელიც წარმოადგენს სუბიექტის მომართვიდან არაუგვიანეს 10 სამუშაო დღეს. ეს ვადა განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთებით შეიძლება გაგრძელდეს არაუმეტეს 10 სამუშაო დღით, რის შესახებაც მონაცემთა სუბიექტს დაუყოვნებლივ ეცნობება წერილობით მართვის სისტემის მიერ.

5. იმ შემთხვევაში, თუ პერსონალურ მონაცემთა დაცვის ოფიცერი მოთხოვნის საფუძვლის, შესაბამისი დასაბუთების და აუდიოჩანაწერის შინაარსის გათვალისწინებით, მიზანშეწონილად არ მიიჩნევს მონაცემთა სუბიექტის მოთხოვნის დაკმაყოფილებას, იგი არაუგვიანეს 10 სამუშაო დღემდე ვადაში, მართვის სისტემის უფროსთან შეთანხმების შემდეგ, მონაცემთა სუბიექტს, წერილობითი ფორმით ატყობინებს გადაწყვეტილებას, შესაბამისი დასაბუთების მითითებით.

6. მონაცემთა სუბიექტი უფლებამოსილია წერილობითი უარის მიღებიდან ერთი თვის ვადაში აღნიშნული გადაწყვეტილება გაასაჩივროს კანონმდებლობით დადგენილი წესით.

7. მონაცემთა სუბიექტის უფლებები შესაძლებელია შეიზღუდოს კანონმდებლობით გათვალისწინებულ შემთხვევებში.

მუხლი 10. მონაცემთა სუბიექტის უფლებების შეზღუდვა

1. გათვალისწინებული უფლებები შეიძლება შეიზღუდოს, თუ ეს პირდაპირ არის გათვალისწინებული საქართველოს კანონმდებლობით, ამით არ ირღვევა ადამიანის ძირითადი უფლებები და თავისუფლებები, ეს არის აუცილებელი და პროპორციული ზომა დემოკრატიულ საზოგადოებაში და ამ უფლებების განხორციელებამ შეიძლება საფრთხე შეუქმნას:

ა) სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს;

ბ) საზოგადოებრივი უსაფრთხოების ინტერესებს;

გ) დანაშაულის თავიდან აცილებას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას, მართლმსაჯულების განხორციელებას, პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას, არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას, ოპერატიულ-სამძებრო საქმიანობას;

დ) ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს;

ე) მონაცემთა სუბიექტის მიერ პროფესიული, მათ შორის, რეგულირებადი პროფესიის, ეთიკის ნორმების დარღვევის გამოვლენას და მისთვის პასუხისმგებლობის დაკისრებას;

ვ) ამ მუხლის პირველი პუნქტის „ა“, „ბ“, „გ“, „დ“, „ე“, „ზ“ ან „ი“ ქვეპუნქტით განსაზღვრულ სფეროებში მარეგულირებელი ან/და ზედამხედველობის განმახორციელებელი ორგანოების ფუნქციებისა და უფლებამოსილებების განხორციელებას;

ზ) მონაცემთა სუბიექტის ან/და სხვა პირების უფლებებსა და თავისუფლებებს, მათ შორის, გამოხატვის თავისუფლებას;

თ) სახელმწიფო, კომერციული, პროფესიული და კანონით გათვალისწინებული სხვა სახის საიდუმლოებების დაცვას;

ი) სამართლებრივი მოთხოვნის ან შესაგებლის დასაბუთებას.

2. მონაცემთა სუბიექტისთვის ამ უფლების გამოყენებაზე უარის შემთხვევაში, მართვის სისტემა მას მიაწვდის წერილობით დასაბუთებას კონკრეტული საფუძვლით უარის თქმის თაობაზე, გარდა იმ შემთხვევისა, თუ ინფორმაციის მიწოდება საფრთხეს შეუქმნის ამ მუხლის პირველი პუნქტით გათვალისწინებული მიზნის (მიზნების) მიღწევას.

მუხლი 11. გასაჩივრების უფლება

1. მონაცემთა სუბიექტს უფლება აქვს, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული უფლებებისა და დადგენილი წესების დარღვევის შემთხვევაში კანონით დადგენილი წესით მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს, სასამართლოს ან/და ზემდგომ ადმინისტრაციულ ორგანოს.
2. მონაცემთა სუბიექტს უფლება აქვს, პერსონალურ მონაცემთა დაცვის სამსახურს მოსთხოვოს მონაცემთა დაბლოკვის შესახებ გადაწყვეტილების მიღება განცხადების განხილვის დასრულების თაობაზე გადაწყვეტილების გამოტანამდე.
3. მონაცემთა სუბიექტს უფლება აქვს, პერსონალურ მონაცემთა დაცვის სამსახურის გადაწყვეტილება გაასაჩივროს სასამართლოში საქართველოს კანონმდებლობით გათვალისწინებული პირობებისა და ვადების დაცვით.

მუხლი 12. მონაცემთა გადაცემა, გამჟღავნება

ვიდეომონიტორინგის შედეგად მოპოვებული მონაცემები შესაბამისი სამართლებრივი საფუძვლის არსებობისას, კანონმდებლობით დადგენილი წესითა და მოცულობით შეიძლება გადაეცეს შემდეგ მესამე პირებს:
ა) სამართალდამცავ ორგანოებს;
ბ) სასამართლოს;
გ) პერსონალურ მონაცემთა დაცვის სამსახურს;
დ) კანონმდებლობით გათვალისწინებულ სხვა ორგანოებს.