იმპორტიორთა მონაცემების უსაფრთხოების დაცვის პოლიტიკა

თავი I. ზოგადი დებულებები, მიზანი და სამართლებრივი საფუძვლები

მუხლი 1. პოლიტიკის მიზანი და რეგულირების სფერო

1. წინამდებარე დოკუმენტი წარმოადგენს ა(ა)იპ - „ქონებრივი უფლებების კოლექტიურ საფუძველზე მმართველი ორგანიზაცია - ინტელექტუალური საკუთრების მფლობელთა ასოციაციის“ (შემდგომში - ასოციაცია) (ს/ნ: 404574475) შიდა სახელმძღვანელო უსაფრთხოების პოლიტიკას. იგი განსაზღვრავს კერძო კოპირების დეპარტამენტში შემოსავლების სამსახურიდან მიღებული საბაჟო ინფორმაციის, ბიზნეს-მონაცემებისა და პერსონალური მონაცემების დაცვის უსაფრთხოების ტექნიკურ და ორგანიზაციულ ზომებს.
2. პოლიტიკის ძირითადი მიზანია შექმნას მკაცრად კონტროლირებადი, დაცული და იზოლირებული სამუშაო გარემო მიღებული საბაჟო მონაცემების დასამუშავებლად. დოკუმენტი უზრუნველყოფს საინფორმაციო ნაკადების უსაფრთხოებას და მიზნად ისახავს ნებისმიერი შიდა თუ გარე საფრთხის, ინფორმაციის გაჟონვის, უნებართვო ასლის გადაღების ან მონაცემთა არასანქცირებული ცვლილების თავიდან აცილებას.
3. წინამდებარე პოლიტიკა ეყრდნობა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონს და „საავტორო და მომიჯნავე უფლებების შესახებ“ საქართველოს კანონს.

მუხლი 2. პერსონალურ მონაცემთა დაცვის ოფიცრის როლი და ზედამხედველობა

1. ასოციაციაში მონაცემთა დამუშავების პროცესებზე მუდმივ კონტროლსა და ზედამხედველობას ახორციელებს პერსონალურ მონაცემთა დაცვის ოფიცერი.
2. მონაცემთა დაცვის ოფიცერი რეგულარულად ამოწმებს კერძო კოპირების დეპარტამენტის მიერ საბაჟო მონაცემთა დამუშავების შესაბამისობას „საავტორო და მომიჯნავე უფლებების შესახებ“ საქართველოს კანონთან, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან, ასოციაციაში სპეციალურად შემუშავებულ და დანერგილ სამართლებრივ დოკუმენტებთან, აგრეთვე, მონაცემთა უსაფრთხოების უზრუნველყოფის საუკეთესო სტანდარტებთან.

თავი II. მონაცემთა უსაფრთხოების ორგანიზაციული და ტექნიკური ზომები

მუხლი 3. დასაქმებულ პირთა მიერ კონფიდენციალურობის დაცვის ვალდებულებები

1. კერძო კოპირების დეპარტამენტის თითოეული თანამშრომელი ვალდებულია სამსახურებრივი მოვალეობის შესრულების დაწყებამდე გაეცნოს წინამდებარე პოლიტიკას და ხელი მოაწეროს ასოციაციაში მოქმედ „ინფორმაციის გაუმჟღავნებლობის შესახებ შეთანხმებას“.

2. დეპარტამენტის ყველა თანამშრომლის შრომითი ხელშეკრულებისა და ინფორმაციის გაუმჟღავნებლობის შესახებ შეთანხმების განუყოფელ პირობას წარმოადგენს მუშაობის პროცესში მოპოვებული, დამუშავებული ან ხელმისაწვდომი ნებისმიერი საბაჟო, ბიზნეს თუ პერსონალური მონაცემის მკაცრი კონფიდენციალურობის დაცვა.

3. დეპარტამენტის თანამშრომლებს ეკრძალებათ სამსახურებრივი საქმიანობისას მიღებული ინფორმაციის ნებისმიერი ფორმით (ზეპირი, წერილობითი, ელექტრონული) გამჟღავნება, გადაცემა, ასლის გადაღება, ფოტო/ვიდეო გადაღება, მატერიალური ან ელექტრონული ფორმით ჩანაწერების გაკეთება ან მესამე პირებისთვის ხელმისაწვდომობის უზრუნველყოფა, გარდა საქართველოს კანონმდებლობითა და ასოციაციის შიდა რეგულაციებით პირდაპირ გათვალისწინებული შემთხვევებისა.

4. წინამდებარე მუხლით განსაზღვრული ინფორმაციის კონფიდენციალურობის დაცვის ვალდებულება უვადოა და ძალაში რჩება თანამშრომლის მიერ ასოციაციაში საქმიანობის შეწყვეტის, შრომითი ურთიერთობის დასრულების ან სამსახურიდან წასვლის შემდგომ ეტაპზეც.

5. მონაცემთა უნებართვო გაზიარება, გამჟღავნება ან უსაფრთხოების წესების უგულებელყოფა იწვევს დისციპლინურ პასუხისმგებლობას ასოციაციის შინაგანაწესის შესაბამისად, რაც შეიძლება გახდეს შრომითი ხელშეკრულების დაუყოვნებლივ შეწყვეტის საფუძველი, აგრეთვე იწვევს საქართველოს კანონმდებლობით გათვალისწინებულ სამოქალაქო, ადმინისტრაციულ ან/და სისხლისსამართლებრივ პასუხისმგებლობას.

მუხლი 4. სამუშაო სივრცეში ფიზიკური დაშვების კონტროლი

1. კერძო კოპირების დეპარტამენტის სამუშაო ოთახი, სადაც ფიზიკურად მიმდინარეობს საბაჟო მონაცემების დამუშავება, წარმოადგენს იზოლირებულ და მკაცრად შეზღუდული დაშვების ზონას.

2. სამუშაო სივრცეში შესვლა და სივრციდან გამოსვლა ხორციელდება ინდივიდუალური ელექტრონული საიდენტიფიკაციო ბარათების საშუალებით.

3. სამუშაო ოთახში დაშვების უფლება აქვთ მხოლოდ კერძო კოპირების დეპარტამენტის თანამშრომლებს. ხოლო საჭიროების შემთხვევაში, ტექნიკური გაუმართაობის აღმოფხვრის მიზნით, კერძო კოპირების დეპარტამენტის უფროსის ნებართვის საფუძველზე, ინფორმაციული ტექნოლოგიების სპეციალისტს.

4. ინდივიდუალური ელექტრონული საიდენტიფიკაციო ბარათების გარეშე ოთახში შესვლა ტექნიკურად შეუძლებელია.

5. სისტემა პირდაპირ არის ინტეგრირებული დეპარტამენტის ხელმძღვანელის მობილურ მოწყობილობასთან, რაც უზრუნველყოფს ოთახში შესვლის კონტროლის შესაძლებლობას.

მუხლი 5. საბაჟო მონაცემთა ბაზაზე წვდომის უფლებამოსილება

1. ელექტრონული საინფორმაციო ბაზა, სადაც ინახება და მუშავდება შემოსავლების სამსახურიდან მიღებული საბაჟო ინფორმაცია, წარმოადგენს მკაცრად შეზღუდული დაშვების ციფრულ სივრცეს.

2. ელექტრონული საინფორმაციო ბაზა, სადაც ინახება და მუშავდება შემოსავლების სამსახურიდან მიღებული საბაჟო ინფორმაცია, წარმოადგენს დაცულ ციფრულ სივრცეს. აღნიშნული ბაზა და მასში არსებული ყველა მონაცემი თავსდება და ინახება ექსკლუზიურად ასოციაციის საკუთარ, ლოკალურ სერვერზე. დასახელებულ სერვერულ ინფრასტრუქტურაზე არანაირი ფორმით არ გააჩნიათ წვდომა გარე მესამე პირებს, რაც მაქსიმალურად ზრდის მონაცემთა უსაფრთხოების დაცვის სტანდარტს და გამორიცხავს არაუფლებამოსილი პირების მხრიდან საინფორმაციო რესურსებზე არასანქცირებული შეღწევის რისკებს.

3. აღნიშნულ მონაცემთა ბაზაზე პირველადი, სრული და ადმინისტრაციული წვდომის უფლებამოსილება გააჩნია კერძო კოპირების დეპარტამენტის უფროსს. დეპარტამენტის სხვა თანამშრომლებს ინფორმაციის მოდიფიცირების უფლება არ აქვთ.

4. სისტემაში მომხმარებელთა აქტივობის მონიტორინგისა და შემდგომი კონტროლის მიზნით, ავტომატურ რეჟიმში, უწყვეტად აღირიცხება ელექტრონული ჟურნალი (ლოგები). სისტემური აღრიცხვის ჟურნალში

ფიქსირდება ბაზაში განხორციელებული თითოეული ავტორიზაციის ზუსტი დრო (თარიღი, საათი და წუთი), სესიის ხანგრძლივობა, აგრეთვე მომხმარებლის მიერ შესრულებული ყოველი კონკრეტული მოქმედება (მონაცემთა ნახვა, ძებნა, ცვლილება, ფილტრაცია თუ სხვაგვარი დამუშავება).

5. ბაზაში არასანქცირებული შეღწევის, არასწორი მონაცემების გამოყენების ან პაროლის ზედიზედ 3 (სამი) შეცდომით შეყვანის მცდელობის შემთხვევაში, სისტემა ავტომატურად ბლოკავს კონკრეტულ მომხმარებელს და წვდომის არხს. აღნიშნულის შესახებ დეპარტამენტის უფროსს და ინფორმაციული ტექნოლოგიების სპეციალისტს ელექტრონული ფოსტის მისამართზე დაუყოვნებლივ ეგზავნება შეტყობინება. ბაზაზე წვდომის განბლოკვა შესაძლებელია მხოლოდ ხელმძღვანელის თანხმობის საფუძველზე ინფორმაციული ტექნოლოგიების სპეციალისტის მიერ.

მუხლი 6. მატერიალური დოკუმენტების უსაფრთხოება

1. ნებისმიერი დოკუმენტი, რომელიც იბეჭდება სამსახურებრივი მიზნებისთვის (ინვოისები, საბაჟო ამონაწერები და სხვა) და შეიცავს კონფიდენციალურ ინფორმაციას, წარმოადგენს მკაცრი დაცვის ობიექტს.

2. ყველა მატერიალური დოკუმენტი სავალდებულო წესით ინახება სპეციალურ რკინის სეიფში, რომლის გასაღები აქვს მხოლოდ დეპარტამენტის უფროსს. საჭიროების შემთხვევაში, დეპარტამენტის უფროსის ნებართვის საფუძველზე, მხოლოდ კერძო კოპირების დეპარტამენტის შესაბამის თანამშრომელს ექნება სეიფზე წვდომის უფლებამოსილება.

3. უსაფრთხოების უზრუნველყოფის მიზნით, აღნიშნული რკინის სეიფიდან დოკუმენტების სამუშაო ოთახის გარეთ გატანა მკაცრად იკრძალება.

4. რკინის სეიფი მუდმივად ჩაკეტილია და მისი გახსნა მხოლოდ საჭიროების შემთხვევაში ხორციელდება.

მუხლი 7. საინფორმაციო ნაკადების მართვა და იერარქიული წვდომა

1. შემოსავლების სამსახურიდან მიღებული საბაჟო მონაცემების გადმოტანას, მათ კორექტირებას, არქივირებასა და თანამშრომელთა შორის სამუშაოს განაწილებას ახორციელებს კერძო კოპირების დეპარტამენტის უფროსი.

2. უსაფრთხოების უზრუნველყოფის მიზნით, დეპარტამენტში მოქმედებს მკაცრი იერარქიული პრინციპი: დეპარტამენტის უფროსის სისტემური ჩართულობისა

და ნებართვის გარეშე, სხვა თანამშრომლებს საბაჟო პირველად ინფორმაციაზე წვდომა არ გააჩნიათ სანამ შესაბამის პროგრამაში არ აიტვირთება.

3. იმ შემთხვევაში, თუკი შემოსავლების სამსახურიდან მიღებული ინფორმაციის დამუშავებისა და იმპორტიორებთან კომუნიკაციის პროცესში წამოიჭრება სამართლებრივი მხარდაჭერის საჭიროება, რაც სცილდება კერძო კოპირების დეპარტამენტის უშუალო კომპეტენციას, პროცესში ერთვება ასოციაციის იურიდიული დეპარტამენტი. იურიდიული დეპარტამენტის ჩართვის, მასალების გადაცემისა და საინფორმაციო ნაკადების უსაფრთხოების წესები დეტალურად რეგულირდება „კერძო კოპირების მიზნებისთვის იმპორტიორთა მონაცემების დამუშავებისა და კონფიდენციალურობის დაცვის წესის“ შესაბამისად.

მუხლი 8. სამუშაო კომპიუტერების ბლოკირება

1. დეპარტამენტის სამუშაო კომპიუტერებზე დანერგილია ავტორიზაციის მრავალდონიანი დამცავი სისტემა. ოპერაციული სისტემის ჩართვა, ჩატვირთვა ან მოწყობილობის ეკრანის განბლოკვა შესაძლებელია შესაბამის კომპიუტერზე ფიზიკურად მიერთებული, წინასწარ ვერიფიცირებული და პერსონალიზებული მატერიალური უსაფრთხოების გასაღების მეშვეობით. აღნიშნულის გარეშე კომპიუტერულ სისტემასთან და მასში არსებულ საინფორმაციო რესურსებთან წვდომა ტექნიკურად შეუძლებელია.

2. დეპარტამენტის სამუშაო კომპიუტერულ მოწყობილობებზე დანერგილია სპეციალიზებული პროგრამული და აპარატურული დამცავი სისტემა, რომელიც მუშაობს სპეციალური ფიზიკური გასაღების პრინციპით.

3. სამუშაო კომპიუტერების საინფორმაციო ბაზა პროგრამულად არის კონტროლირებადი და დახურული. კომპიუტერები არ აღიქვამს სხვა უცხო გარე მეხსიერების ბარათს. აღნიშნული მექანიზმით სრულად გამორიცხულია დეპარტამენტთან არსებული კომპიუტერებიდან ინფორმაციის ფიზიკურად წაღება (გადმოწერა) ან გარედან უცხო ფაილების შემოტანა.

მუხლი 9. ინტერნეტთან წვდომის შეზღუდვა

1. კერძო კოპირების დეპარტამენტის სამუშაო კომპიუტერულ მოწყობილობებზე ინტერნეტთან წვდომა მაქსიმალურად შეზღუდულია, რაც მნიშვნელოვნად ამცირებს მონაცემთა უსაფრთხოების დარღვევის რისკებს.

2. სამუშაო კომპიუტერულ მოწყობილობებზე მხოლოდ იმ ვებგვერდებზე წვდომაა დაშვებული, რაც კრიტიკულად აუცილებელია სამსახურებრივი მოვალეობის შესასრულებლად.

მუხლი 10. მონაცემთა შენახვის ვადები

1. შემოსავლების სამსახურიდან მიღებულ საბაჟო ინფორმაციას, ბიზნეს-მონაცემებს და პერსონალურ მონაცემებს, როგორც ელექტრონული (ლოკალურ სერვერებსა და ციფრულ ბაზებში განთავსებული), ისე მატერიალური ფორმით, ასოციაცია ინახავს იმ ვადით, რაც აუცილებელია ინფორმაციის დამუშავების მიზნის მისაღწევად და საქართველოს კანონმდებლობით ნაკისრი ვალდებულებების სრულად შესასრულებლად, მაგრამ არაუმეტეს 5 (ხუთი) წლის ვადით, გარდა იმ შემთხვევისა როდესაც მონაცემთა შენახვა აუცილებელია მიმდინარე სასამართლო დავის, სააღსრულებო საქმისწარმოების, ადმინისტრაციული წარმოების ან კანონით დადგენილი სხვა სახელშეკრულებო თუ არასახელშეკრულებო ვალდებულებების შესასრულებლად.
2. ამ მუხლის პირველ პუნქტში მითითებული 5 (ხუთი) წლიანი ვადის ამოწურვის შემდგომ, ელექტრონული მონაცემების ბაზებიდან წაშლა/არქივირება და მატერიალური დოკუმენტების განადგურება ხორციელდება ასოციაციის მიერ დადგენილი შიდა პროცედურებისა და უსაფრთხოების წესების დაცვით.
3. იმ შემთხვევაში თუკი 5 (ხუთი) წლიანი ვადის გასვლის შემდეგ სახეზე გვაქვს ამ მუხლის პირველი პუნქტით გათვალისწინებული სასამართლო დავა, სააღსრულებო საქმისწარმოება, ადმინისტრაციული წარმოება და/ან სხვა სახელშეკრულებო თუ არასახელშეკრულებო ვალდებულება, მონაცემები ინახება საქმისწარმოების სრულად დასრულებამდე, რის შემდეგაც, ასოციაცია მიმართავს ამავე მუხლის მე-2 პუნქტით გათვალისწინებულ ღონისძიებებს.

თავი III. მომხმარებელთა ავტორიზაცია და ინფორმაციული ტექნოლოგიების მართვა

მუხლი 10. მომხმარებლის ანგარიშებისა და პაროლების დაცულობა

1. პროგრამულ ბაზაში შესასვლელად დეპარტამენტის ყოველ თანამშრომელს აქვს ინდივიდუალური ანგარიში და პერსონალური, რთული შემადგენლობის პაროლი. პაროლების სხვა პირზე გაზიარება ან კოლეგის ანგარიშით სარგებლობა კატეგორიულად აკრძალულია.

2. სისტემაში შესვლისას პაროლის ზედიზედ 3 (სამი) შეცდომით შეყვანის შემთხვევაში, მომხმარებლის ანგარიში უსაფრთხოების მიზნით ავტომატურად იბლოკება.

3. ანგარიშის განბლოკვა ან პაროლის აღდგენა დავიწყების შემთხვევაში შეუძლებელია განხორციელდეს დისტანციურად ან ონლაინ რეჟიმში. აღნიშნული პროცედურა სრულდება მხოლოდ ადგილობრივად, უშუალოდ იმ ფიზიკურ სერვერზე, სადაც განთავსებულია საავტორიზაციო ბაზა.

4. თუ ბაზაში შესული თანამშრომელი 10 (ათი) წუთის განმავლობაში არ განახორციელებს არანაირ მოქმედებას, სისტემა უსაფრთხოების მიზნით ავტომატურად თიშავს მიმდინარე სესიას და ინფორმაციაზე ხელახალი წვდომის მისაღებად მოითხოვს ხელახალ ავტორიზაციას, ხოლო 1 (ერთი) საათის შემდეგ პროგრამა გადადის „არააქტიურ რეჟიმში“ (Sleep mode).

მუხლი 11. ინფორმაციული ტექნოლოგიების (IT) პერსონალის წვდომის ფარგლები

1. ასოციაციის ინფორმაციული ტექნოლოგიების (IT) სპეციალისტს არ გააჩნია კერძო კოპირების მონაცემთა ბაზაში არსებულ შინაარსობრივ ინფორმაციაზე (იმპორტიორთა კონკრეტულ ფინანსურ, საბაჟო და პერსონალურ მონაცემებზე) წვდომის უფლება.

2. ინფორმაციული ტექნოლოგიების სპეციალისტის კომპეტენცია შემოიფარგლება სისტემების ტექნიკური გამართულობის, ქსელური ინფრასტრუქტურის მუშაობისა და უსაფრთხოების გარე პერიმეტრის მონიტორინგით, ბაზებში შეღწევის უფლების გარეშე.

მუხლი 12. სისტემური ჟურნალების მონიტორინგი და ინციდენტების შეტყობინება

1. მთლიანი საინფორმაციო ინფრასტრუქტურის ტექნიკური მონიტორინგისთვის გამოიყენება სპეციალიზებული პროგრამული სისტემა, რომელიც უწყვეტ რეჟიმში აკონტროლებს სერვერების მუშაობას.

2. ნებისმიერი სახის გარე შეტევის, არასანქცირებული წვდომის მცდელობის ან სისტემური გაუმართაობის დაფიქსირების შემთხვევაში, უსაფრთხოების დამცავი მექანიზმის საშუალებით, მყისიერი რეაგირების მიზნით, ასოციაციის ინფორმაციული ტექნოლოგიების სპეციალისტს ავტომატურად ეგზავნება შეტყობინება ელექტრონულ ფოსტაზე.

თავი IV. დასკვნითი დებულებები

მუხლი 13. პოლიტიკის აღსრულება და პასუხისმგებლობა

1. წინამდებარე პოლიტიკით გათვალისწინებული უსაფრთხოების ტექნიკური ან ორგანიზაციული ზომების უგულებელყოფა, პაროლების ან წვდომის უფლებების მესამე პირებისთვის გაზიარება, ან ბლოკირების მექანიზმების გვერდის ავლის მცდელობა განიხილება საინფორმაციო უსაფრთხოების უხეშ დარღვევად.
2. აღნიშნული ქმედება იწვევს მკაცრ დისციპლინურ პასუხისმგებლობას ასოციაციის შინაგანაწესის შესაბამისად.
3. ასოციაცია გეგმურად, ყოველ ერთ წელში ერთხელ სისტემატურად უზრუნველყოფს წინამდებარე პოლიტიკის დოკუმენტის გადახედვასა და საჭიროების შემთხვევაში მასში შესაბამისი ცვლილებების შეტანას, გარდა იმ შემთხვევისა, როდესაც დოკუმენტის გადახედვისა და მასში ცვლილების შეტანის აუცილებლობა გამოწვეულია სხვა ობიექტური მიზეზებით (მაგალითად, კანონმდებლობის ცვლილება, დამატებითი ორგანიზაციულ-ტექნიკური დამცავი ზომების მიღების აუცილებლობა და სხვა). ასეთ შემთხვევაში, პოლიტიკის გადახედვა (არაგეგმური) და მასში ცვლილებების შეტანა განხორციელდება ასეთი გარემოების დადგომიდან გონივრულ ვადაში.