შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“

ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტი

ინფორმაციული უსაფრთოების პოლიტიკის დოკუმენტი დამტკიცებულია კომპანიის დირექტორის, გიორგი აბრამიშვილის მიერ

2025

სარჩევი

შპს სი-სი-ი-ეიჩ ჰაიდრო VI
ინფორმაციული უსაფრთხოების პოლიტიკა

შესავალი

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ (შემდგომში - „კომპანია“) გურიის რეგიონში, ოზურგეთის მუნიციპალიტეტის ტერიტორიაზე, კერძოდ მდინარე ბახვისწყალზე ახორციელებს ჯამური 10.9 მგვტ დადგმული სიმძლავრის, ბუნებრივ ჩამონადენზე მომუშავე „ბახვი 1“ ჰესის მშენებლობას. კომპანიის ინვესტორები არიან „კავკასიის განახლებადი ენერგიის ჰოლდინგი“ (სი-სი-ი-ეიჩ), ავსტრიული საინვესტიციო ფონდი „ილაგი“ და სხვა სპეციალიზებული ინვესტორები ავსტრიიდან და საქართველოდან. „კავკასიის განახლებადი ენერგიის ჰოლდინგის“ ინვესტორები კი თავის მხრივ, არიან ცნობილი საერთაშორისო საფინანსო ინსტიტუტები ამერიკიდან და ევროპული ქვეყნებიდან (მათ შორის - ევროპის საინვესტიციო ბანკი [EIB], ჰოლანდიის განვითარების ბანკი [FMO], ავსტრიის განვითარების ბანკი [OeEB] და სხვა). აღსანიშნავია, რომ ავსტრიული საინვესტიციო ფონდი „ილაგი“ ფლობს მრავალფეროვან ბიზნეს პორტფელს რამდენიმე დასავლურ ქვეყანაში.

ბახვი 1 ჰესის მშენებლობა მიმდინარეობს მდ.ბახვისწყლის 1 735 და 1 383 მ ნიშნულებს შორის მოქცეულ მონაკვეთზე. გათვალისწინებულია მდ.ბახვისწყლის ბუნებრივ ჩამონადენზე მომუშავე ჰესის მშენებლობა, რომლის შემადგენლობაშია სათავე ნაგებობა, სადაწნეო მილსადენი და მიწისზედა ჰესის შენობა. ჰესის დადგმული სიმძლავრე იქნება 10.9 მგვტ, ხოლო საპროექტო ხარჯი - 4მ^3/წმ. სათავე ნაგებობა განთავსდება მდ.ბახვისწყლისა და მდ.ბაისურას ღელეს შესართავიდან 250 მ-ით ქვემოთ. შეტბორვის დონეა ზღვის დონიდან 1731.70 მ, ხოლო ჰესის შენობის ქვედა ბიეფის ნიშნული ზღვის დონიდან - 1383.0 მ.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI” საკუთარ საქმიანობას წარმართავს საერთაშორისო საფინანსო ინსტიტუტების IFC-ისა და EIB-ის მიერ დადგენილი გარემოსდაცვით და სოციალურ სტანდარტებთან სრული შესაბამისობით.

მიზანი

მოცემული პოლიტიკის დოკუმენტის მიზანია კომპანიის ინფორმაციისა და მასთან დაკავშირებული სისტემების, მათ შორის პერსონალური მონაცემების დაცვის ერთიანი მიდგომის განსაზღვრა.

მოცემულ დოკუმენტში ასახული დებულებები ვრცელდება კომპანიის მიერ დამუშავებულ ყველა სახის ციფრულ და ფიზიკურ ინფორმაციაზე. იგი მოიცავს მონაცემთა მართვასთან დაკავშირებულ პროცესებს, მართვის სისტემებს (მაგ: SCADA - ზედამხედველობის, მართვისა და მონაცემთა შეგროვების სისტემა) და საკომუნიკაციო საშუალებებს. ასევე, ეხება მესამე მხარის მიერ მონაცემთა გამოყენებასთან დაკავშირებულ საკითხებს.

აღნიშნული პოლიტიკა ვრცელდება ყველა თანამშრომელზე, კონტრქტორზე, სერვისის მომწოდებელზე და ნებისმიერ მესამე მხარეზე, მათ შორის კონსულტანტებზე, აუდიტორებზე, მარეგულირებელ ორგანოებზე, ინვესტორებზე, რომელთაც აქვთ წვდომა შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“-ს ინფორმაციაზე, სისტემებსა და ინფრასტრუქტურაზე.

ინფორმაციული უსაფრთხოების პოლიტიკა ასევე აერთიანებს შესაბამისობის პოლიტიკით განსაზღვრულ მოთხოვნებსა და ვალდებულებებს, მათ შორის ინფორმაციის კონფიდენციალურობის დაცვას, სისტემების უსაფრთხოების უზრუნველყოფას, ინციდენტების შეტყობინებას და ადგილობრივი თუ საერთაშორისო სამართლებრივი მოთხოვნების დაცვას.

ინფორმაციული უსაფრთხოება

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ ინფორმაციულ უსაფრთხოებას განსაზღვრავს, როგორც მონაცემების დაცვის პროცესს, რომლის მიზანია მათი კონფიდენციალურობის, სიზუსტისა და ხელმისაწვდომობის უზრუნველყოფა.

ეს მიდგომა ვრცელდება კომპანიის მიერ გამოყენებულ ყველა სახის ინფორმაციასა და ჩანაწერზე მიუხედავად იმისა, ინახება ფიზიკურად ადგილზე, დისტანციურ პლატფორმებზე, თუ გარე სერვისის მომწოდებლების მიერ. იგი ასევე მოიცავს როგორც ციფრულ, ისე ფიზიკურ ფორმატში არსებულ ინფორმაციას და მის მართვასთან დაკავშირებულ პროცესებს. კომპანია ინფორმაციულ უსაფრთხოებას მიიჩნევს საქმიანობის ერთ-ერთ საფუძვლად, რადგან იგი ხელს უწყობს სამართლებრივი მოთხოვნების შესრულებას, სენსიტიური მონაცემების დაცვას და პარტნიორების, მარეგულირებელი ორგანოებისა და ინვესტორების ნდობის შენარჩუნებას.

ენერგეტიკისა და ინფრასტრუქტურის სფეროებში ინფორმაციის უსაფრთხო მართვის მნიშვნელობის გათვალისწინებით, შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ აყალიბებს და აუმჯობესებს ინფორმაციული უსაფრთხოების მიდგომებს საერთაშორისოდ აღიარებული კარგი პრაქტიკისა და არსებული დარგობრივი სტანდარტების შესაბამისად, მათ შორის კრიტიკული ინფრასტრუქტურისთვის მოქმედი მოთხოვნების გათვალისწინებით. ეს მიდგომები მორგებულია კომპანიის მასშტაბზე, საქმიანობის თავისებურებებზე და ციფრული ტექნოლოგიების გამოყენებაზე, როგორც ადმინისტრაციულ, ისე ტექნიკურ პროცესებში.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“-თვის ინფორმაციული უსაფრთხოება მხოლოდ ტექნიკურ საკითხს არ წარმოადგენს. იგი მოიცავს უსაფრთხოების უზრუნველყოფასთან დაკავშირებულ საქმიანობას, მათ შორის წვდომის კონტროლს, თანამშრომელთა ცნობიერების ამაღლებას, ობიექტების ფიზიკურ დაცვას, დადგენილი პროცედურების დაცვას და სისტემებში არსებული სისუსტეების რეგულარულ შეფასებას. კომპანია ინფორმაციულ უსაფრთხოებას უზრუნველყოფს ერთმანეთთან დაკავშირებული დაცვის მექანიზმების ერთობლიობით. შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ მუდმივად აუმჯობესებს მიდგომებს ტექნოლოგიური, რეგულაციური და საოპერაციო რისკების ცვლილებების გათვალისწინებით.

ინფორმაციული უსაფრთხოების მართვა

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“-ში ინფორმაციული უსაფრთხოების მიმართულებას ხელმძღვანელობს კომპანიის დირექტორი, ხოლო შიდა კოორდინაციას უზრუნველყოფს გარემოსდაცვითი, სოციალური და მმართველობითი მენეჯერი. სტრატეგიის დონეზე განსაზღვრული პასუხისმგებლობა ეკისრება კომპანიის ხელმძღვანელობას. ტექნიკური დაცვის უზრუნველყოფასა და კიბერუსაფრთხოების ზომების გატარებაზე პასუხისმგებელია შესაბამისი კვალიფიკაციის მქონე გარე სერვისის მომწოდებელი, მასთან გაფორმებული ხელშეკრულების საფუძველზე.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ აღიარებს, რომ ინფორმაციული უსაფრთხოება წარმოადგენს სამართლებრივი მოთხოვნების შესრულების, სისტემების საიმედო მუშაობისა და დაინტერესებული მხარეების ნდობის მნიშვნელოვან საფუძველს. შესაბამისად, ეს მიმართულება ორგანიზებულია ისე, რომ კომპანიის საქმიანობის ყველა მიმართულებით უზრუნველყოფილი იყოს პასუხისმგებლობის მკაფიო განაწილება, როლების სიცხადე და კარგი პრაქტიკის ერთგვაროვანი გამოყენება. აღნიშნული მიზნად ისახავს არა მხოლოდ მონაცემების დაცვას, არამედ საქმიანობის მდგრადობას და მუდმივად ცვალებად გარემოში სამართლებრივ მოთხოვნებთან შესაბამისობას.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ მონაცემთა კონფიდენციალურობასა და კიბერუსაფრთხოებას უზრუნველყოფს ყოვლისმომცველი და რისკების გათვალისწინებაზე დაფუძნებული მიდგომით. კომპანია უზრუნველყოფს, რომ პერსონალური და ოპერირების პროცესებთან დაკავშირებული მონაცემები მუშავდებოდეს კანონიერად, სამართლიანად და განსაზღვრული მიზნებისათვის, პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის შესაბამისად. კომპანია იყენებს მონაცემთა შენახვისა და წვდომის მკაცრ წესებს და უზრუნველყოფს, რომ ნებისმიერი პირი ინფორმირებული იყოს მის მონაცემებთან დაკავშირებული უფლებების შესახებ. განსაკუთრებული კატეგორიის მონაცემები, მათ შორის მონაცემები ჯანმრთელობის მდგომარეობასთან და ან ზოგადად ჯანმრთელობასთან დაკავშირებით, მუშავდება მხოლოდ

შესაბამისი სამართლებრივი საფუძვლის ან წერილობითი თანხმობის არსებობის შემთხვევაში. მართვის მექანიზმები უზრუნველყოფს, რომ აღნიშნული პრინციპები დაცულია როგორც დოკუმენტალურად, ისე ყოველდღიურ საქმიანობაში.

კიბერუსაფრთხოების მართვა მოიცავს შემდეგ ძირითად ღონისძიებებს:

- კომპიუტერულ სისტემებზე საზიანო პროგრამებისგან დაცვის საშუალებების გამოყენებას და მათი რეგულარულ განახლებას;
- ძლიერი პაროლების გამოყენებას და სისტემაში შესვლისას დამატებითი დადასტურების მოთხოვნას;
- მონაცემთა სარეზერვო ასლების შექმნას, მათ უსაფრთხო შენახვას და პერიოდულ შემოწმებას;
- მონაცემებზე წვდომის განსაზღვრას თანამშრომლის როლის მიხედვით და სამუშაო მოწყობილობების დაცვას;
- სამუშაო გარემოში დადგენილი წესების დაცვას და უსაფრთხო საკომუნიკაციო საშუალებების გამოყენებას;
- ინფორმაციული ტექნოლოგიების დამოუკიდებელი სპეციალისტის მიერ კიბერუსაფრთხოების ზომების პერიოდულ გადახედვას ახალი საფრთხეების დროულად გამოვლენის მიზნით.

ინფორმაციული უსაფრთხოების პოლიტიკის ჩარჩო გადაიხედება ყოველწლიურად ან მაშინ, როდესაც ადგილი აქვს მნიშვნელოვან ცვლილებებს კანონმდებლობაში, გამოყენებულ სისტემებში ან რისკებთან დაკავშირებულ გარემოებებში. ასეთი ცვლილებები შეიძლება მოიცავდეს პროგრამული უზრუნველყოფის განახლებას, ახალი სამუშაო ინსტრუმენტების დანერგვას, გარე სერვისის მომწოდებლების ჩართვას ან მონაცემთა მართვასთან დაკავშირებული სამართლებრივი მოთხოვნების ცვლილებას. განახლებული პოლიტიკა ოფიციალურად მტკიცდება კომპანიის დირექტორის მიერ და ვრცელდება თანამშრომლებზე მისი გაცნობისა და შესრულების მიზნით. შემდგომ ტარდება შესაბამისი ტრენინგები ან სამუშაო შეხვედრები.

მართვისა და ანგარიშგების ძირითადი მექანიზმები მოიცავს:

- **მონაცემთა უსაფრთხოების დარღვევის, ან კიბერუსაფრთხოების ინციდენტის შემთხვევაში** დაუყოვნებლივ ინფორმაციის მიწოდებას კომპანიის დირექტორისა და გარემოსდაცვითი, სოციალური და მმართველობითი მენეჯერისთვის. განსაკუთრებით მაშინ, როდესაც ინციდენტი ეხება მართვის სისტემებს, ოპერირების ქსელებს, ან სენსიტიურ მონაცემებს. ინციდენტის შემდეგ უზრუნველყოფილია მისი დოკუმენტირება, მიზეზების დადგენა და ინფორმაციული ტექნოლოგიების დამოუკიდებელ სპეციალისტთან კოორდინაცია, როგორც პრობლემის აღმოსაფხვრელად, ისე სისტემების აღსადგენად. აღნიშნული პროცესი მნიშვნელოვანია შეუფერხებელი მუშაობისა და მონაცემთა დაცვის მოთხოვნების შესრულების უზრუნველსაყოფად;
- **დამოუკიდებელი, მესამე მხარის სპეციალისტთან ერთად პერიოდულად ტარდება სისტემების გამართულობისა და მოთხოვნებთან შესაბამისობის შეფასება,** ჰიდროელექტროსადგურის მუშაობისთვის მნიშვნელოვანი მაჩვენებლების გათვალისწინებით. ეს მოიცავს მართვის სისტემებზე წვდომის ჩანაწერების გადამოწმებას, შესაძლო საფრთხეების მიმოხილვას, პროგრამების განახლების მდგომარეობის შეფასებას, სისტემების გამართულობის შემოწმებას და სისტემებში დაფიქსირებული არასტანდარტული მოქმედებების ანალიზს. ასეთი შეფასებები

ამცირებს ოპერირების ხარვეზებს და ხელს უწყობს ჰიდროელექტროსადგურის შეუფერხებელ მუშაობას, განსაკუთრებით მაშინ, როდესაც ტექნოლოგიური პროცესების მართვა და ინფორმაციის დამუშავება ერთმანეთთან მჭიდროდ არის დაკავშირებული.

მესამე მხარის ინფორმაციული ტექნოლოგიების სერვისის მომწოდებელი ვალდებულია დაიცვას ხელშეკრულებით განსაზღვრული უსაფრთხოების მოთხოვნები, მათ შორის წვდომის კონტროლი, მონაცემთა დაცვა, პროგრამების დროული განახლება და ინციდენტებზე რეაგირება. მისი საქმიანობა რეგულარულად ფასდება კომპანიის რისკების მართვისა და შესაბამისობის სისტემის ფარგლებში.

ინფორმაციული უსაფრთხოების ზედამხედველობას კურირებს კომპანიის დირექტორი, რაც უზრუნველყოფს საკითხის ინტეგრირებას გადაწყვეტილებების მიღების პროცესში და ასახავს კომპანიის ვალდებულებას სამართლებრივი მოთხოვნების შესრულების, საქმიანობის უწყვეტობისა და კარგი მართვის პრინციპების მიმართ.

ინფორმაციული უსაფრთხოების პოლიტიკა

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“-მა შეიმუშავა ინფორმაციული უსაფრთხოების ყოვლისმომცველი პოლიტიკა, რომლის მიზანია კომპანიის ინფორმაციის, პერსონალური და საოპერაციო მონაცემებისა და ჰიდროელექტროსადგურის ფუნქციონირებისთვის გამოყენებული ტექნოლოგიების დაცვა. პოლიტიკა ჩამოყალიბებულია ისე, რომ უზრუნველყოფდეს შესაბამისობას როგორც პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონთან, ისე საერთაშორისო აღიარებულ სტანდარტებსა და პრაქტიკასთან, რომლებიც ვრცელდება კრიტიკული ინფრასტრუქტურისა და ენერგეტიკის სფეროზე.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ აცნობიერებს, რომ ინფორმაციული უსაფრთხოების უზრუნველყოფა ეხება არა მხოლოდ კომპანიის შიდა საქმიანობას, არამედ თანამშრომლებს, კონტრაქტორებს, დამოუკიდებელი მესამე მხარის სერვისის მომწოდებლებს და სხვა პირებს, რომელთაც აქვთ წვდომა კომპანიის სისტემებზე. პოლიტიკა განსაზღვრავს როგორც პრევენციულ, ისე რეაგირების ზომებს და ასახავს კომპანიის ვალდებულებას სამართლებრივი მოთხოვნების შესრულების, საქმიანობის უწყვეტობისა და დაინტერესებული მხარეების ნდობის მიმართ.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“-ს აქვს კიბერუსაფრთხოების პროგრამა, რომლის მიზანია პერსონალურ და ოპერირების მონაცემებზე არასანქცირებული წვდომის, მათი დაკარგვის ან არასწორი გამოყენების პრევენცია. პროგრამა ხორციელდება დამოუკიდებელი, მესამე მხარის ინფორმაციული ტექნოლოგიების სპეციალისტთან თანამშრომლობით და მოიცავს შემდეგ ღონისძიებებს:

- კომპიუტერული სისტემების დაცვას საზიანო პროგრამებისგან და დაცვის საშუალებების რეგულარულ განახლებას;
- ძლიერი და უნიკალური პაროლების გამოყენებას და სისტემაში შესვლისას დამატებითი დადასტურების მოთხოვნას;
- მონაცემთა სარეზერვო ასლების შექმნას და მათ უსაფრთხო შენახვას დისტანციურ პლატფორმებზე;
- მონაცემებზე წვდომის განსაზღვრას თანამშრომლის როლის მიხედვით და ინდივიდუალური მომხმარებლის მონაცემების გამოყენებას;
- სამუშაო მოწყობილობების დაცვას, მათ შორის პაროლების გამოყენებას და ეკრანის ავტომატურ დაბლოკვას;
- კონფიდენციალურობის დაცვის წესების დაცვას, მათ შორის საკომუნიკაციო საშუალებების გამოყენებას;

- უსაფრთხოების წესების, სისტემების პარამეტრებისა და მომხმარებლის წვდომის უფლებების პერიოდულ გადახედვას.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ ასევე იყენებს მკაცრ ზომებს ფიზიკური ფორმით არსებული ინფორმაციის დასაცავად, მათ შორის ბეჭდური დოკუმენტების, ოპერირებასთან ჩანაწერებისა და ქაღალდზე დატანილი მასალების მიმართ. ყველა სენსიტიური, ან კონფიდენციალური დოკუმენტი უნდა ინახებოდეს ჩაკეტილ კარადებში, ან კონტროლირებადი წვდომის მქონე არქივებში და ხელმისაწვდომი იყოს მხოლოდ უფლებამოსილი პირებისთვის. კომპანია ადგენს სამუშაო სივრცეში წესრიგის დაცვას, რაც გულისხმობს, რომ თანამშრომლებმა სამუშაო დასრულების შემდეგ არ დატოვონ მაგიდაზე კონფიდენციალური, ან პერსონალური მონაცემების შემცველი დოკუმენტები. დოკუმენტები, რომლებიც აღარ არის საჭირო, უნდა განადგურდეს უსაფრთხო მეთოდებით (მაგალითად, დაქუცმაცებით) კომპანიის შიდა წესების შესაბამისად, რომლებიც არეგულირებს მონაცემთა შენახვასა და განადგურებას.

შესაბამისობის პოლიტიკის შესაბამისად, ყველა თანამშრომელი, კონტრაქტორი და მესამე მხარის წარმომადგენელი ვალდებულია ხელი მოაწეროს კონფიდენციალურობის შეთანხმებას და დაიცვას ინფორმაციული სისტემების გამოყენების წესები, როგორც კომპანიის სისტემებსა და ობიექტებზე წვდომის აუცილებელი პირობა. აღნიშნული შეთანხმებები იურიდიულად სავალდებულოა და განსაზღვრავს პასუხისმგებლობას მონაცემების გამოყენების, სისტემებით სარგებლობისა და ეთიკური ქცევის მიმართულებით. ინფორმაციული უსაფრთხოების პოლიტიკის დარღვევა, მათ შორის არასანქცირებული წვდომის მცდელობა, მომხმარებლის მონაცემების გაზიარება ან დაუშვებელი პროგრამების გამოყენება, ექვემდებარება შიდა განხილვას და შესაბამის სანქციებს, რაც შეიძლება მოიცავდეს ხელშეკრულების შეწყვეტას.

ჰიდროელექტროსადგურის მართვის სისტემები, რომლებიც უზრუნველყოფს პროცესების რეალურ დროში კონტროლსა და მონიტორინგს, იზოლირებულია საჯარო ინტერნეტისგან როგორც ტექნიკურად, ისე პროგრამულად. ამ სისტემებზე წვდომა აქვს მხოლოდ განსაზღვრულ ტექნიკურ პერსონალს და საქმიანობა ხორციელდება მკაცრად კონტროლირებულ პირობებში. ამ სისტემებზე წვდომა და მათში შეტანილი ცვლილებები აღირიცხება და შემდგომ მოწმდება როგორც კომპანიის შიდა პასუხისმგებელი პირების მიერ, ისე დამოუკიდებელი მესამე მხარის ინფორმაციული ტექნოლოგიების სპეციალისტის მიერ.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ ასევე განსაკუთრებულ ყურადღებას უთმობს პერსონალური მონაცემების დაცვასა და მათ სწორ გამოყენებას. დამუშავებული მონაცემები, მათ შორის საკონტაქტო, ფინანსური და ტექნიკური ინფორმაცია, ინახება უსაფრთხოდ და მხოლოდ იმ ვადით, რაც აუცილებელია შესაბამისი მიზნების მისაღწევად, ან კანონით განსაზღვრული მოთხოვნების შესასრულებლად. ასეთ მონაცემებზე წვდომა განისაზღვრება თანამშრომლის როლის მიხედვით, ხოლო განსაკუთრებული კატეგორიის მონაცემების (მაგალითად, ჯანმრთელობასთან დაკავშირებული ინფორმაციის) გამოყენება დასაშვებია მხოლოდ შესაბამისი სამართლებრივი საფუძვლის ან დადასტურებული თანხმობის არსებობის შემთხვევაში.

ჰესის ოპერირების თითოეულ ობიექტებზე ვიდეომეთვალყურეობა ხორციელდება შეზღუდულად და მხოლოდ დასაბუთებული საჭიროების ფარგლებში. თანამშრომლები და ვიზიტორები წინასწარ არიან ინფორმირებულნი ვიდეომეთვალყურეობის შესახებ, მოქმედი მონაცემთა დაცვის მოთხოვნების შესაბამისად.

კომპანიაში მოქმედებს მონაცემთა შენახვისა და განადგურების განსაზღვრული წესები. მონაცემები, რომლებიც აღარ არის საჭირო, უსაფრთხოდ იშლება, ან ინახება არქივში. მონაცემები არ იშლება მხოლოდ იმ შემთხვევაში, თუ მათი შენახვა აუცილებელია კანონით განსაზღვრული ვალდებულებების შესასრულებლად (მაგალითად, საგადასახადო ან გარემოსდაცვითი მოთხოვნები).

აღნიშნული მიდგომების შედეგად, შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ უზრუნველყოფს ინფორმაციისა და პერსონალური მონაცემების დაცვას არასანქცირებული წვდომის, არასწორი გამოყენებისა და დაკარგვისგან, რაც აძლიერებს კომპანიის ვალდებულებას კარგი მართვის, საქმიანობის ეფექტიანობისა და სამართლებრივი მოთხოვნების შესრულების მიმართ.

ინფორმაციული უსაფრთხოების მართვის სისტემა

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“-ში დანერგილია ინფორმაციული უსაფრთხოების მართვის სისტემა, რომლის მიზანია ჰიდროელექტროსადგურის უსაფრთხო და შეუფერხებელი ფუნქციონირების უზრუნველყოფა. სისტემა მუშაობს ინფორმაციული ტექნოლოგიების დამოუკიდებელ სპეციალისტთან თანამშრომლობით და მორგებულია ენერგეტიკის სექტორისთვის დამახასიათებელ რისკებსა და საქართველოს მოქმედ რეგულაციებზე.

ინფორმაციული უსაფრთხოების მართვის სისტემა ეფუძნება ეტაპობრივ ციკლს, რომელიც მოიცავს დაგეგმვას, განხორციელებას, შემოწმებას და შემდგომ გაუმჯობესებას. ეს მიდგომა უზრუნველყოფს სისტემის უწყვეტ განვითარებას და მის ადაპტირებას მიმდინარე მოთხოვნებსა და ცვლილებებთან. სისტემა მოიცავს არა მხოლოდ ინფორმაციის დაცვას, არამედ ტექნოლოგიური პროცესების მართვასთან დაკავშირებულ რისკებსაც, მათ შორის ჰიდროელექტროსადგურის მუშაობისთვის მნიშვნელოვან მართვის სისტემებს და მათთან დაკავშირებულ მოწყობილობებს.

ინფორმაციული უსაფრთხოების მართვის სისტემა მოიცავს შემდეგ ძირითად ნაწილებს:

- **კომპანიის აქტივების განსაზღვრასა და აღრიცხვას**, რომელიც მოიცავს როგორც ციფრულ, ისე ფიზიკურ აქტივებს, მათ შორის კომპიუტერულ მოწყობილობებს, მართვის სისტემებს, მონაცემთა საცავებს, ადგილზე გამოყენებულ მოწყობილობებს, ასევე ბეჭდურ დოკუმენტებსა და სამუშაო ჩანაწერებს. თითოეული მათგანი აღირიცხება და კონტროლდება მათი მნიშვნელობისა და კრიტიკულობის მიხედვით;
- **რისკების გამოვლენასა და შეფასებას**, რომელიც მორგებულია ჰიდროელექტროსადგურის საქმიანობის თავისებურებებზე და მოიცავს კიბერუსაფრთხოებასთან დაკავშირებულ საფრთხეებს (მაგალითად, საზიანო პროგრამებს ან სისტემებზე არასანქცირებული წვდომის მცდელობებს), ფიზიკურ რისკებს (მაგალითად, უნებართვო შეღწევას ან დოკუმენტების დაკარგვას) და მესამე მხარესთან დაკავშირებულ რისკებს (მაგალითად, სერვისის მომწოდებლების მიერ სისტემებზე წვდომას);
- **შესაძლო საფრთხეების ანალიზსა და შესაბამისი რეაგირების გეგმების შემუშავებას**, მესამე მხარის ინფორმაციული ტექნოლოგიების სპეციალისტთან თანამშრომლობით. ეს გეგმები ეფუძნება რეალურ სცენარებს, რომლებიც შეიძლება გავლენას ახდენდეს ელექტროენერგიის წარმოებაზე, მონაცემთა უსაფრთხოებაზე, ან სამართლებრივი მოთხოვნების შესრულებაზე და მიზნად ისახავს შეფერხების შემცირებას;
- სისტემების პერიოდულ შემოწმებას და მიღებული შედეგების შეფასებას, რაც მოიცავს შიდა წესების გადახედვას, სისტემების მდგომარეობის შეფასებას და მოქმედ სამართლებრივ მოთხოვნებთან და ფინანსური ინსტიტუტების პირობებთან შესაბამისობის დადასტურებას;
- სისტემის მუდმივ გაუმჯობესებასა და პერიოდულ გადახედვას კომპანიის დირექტორისა და გარემოსდაცვითი, სოციალური და მმართველობითი მენეჯერის მონაწილეობით, მესამე მხარის ინფორმაციული ტექნოლოგიების სპეციალისტისა. პოლიტიკა გადაიხედება არანაკლებ წელიწადში ერთხელ და მოიცავს ინციდენტების ჩანაწერების, შესრულების მაჩვენებლებისა და მოსალოდნელი მარეგულირებელი ცვლილებების განხილვას.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“-ის ინფორმაციული უსაფრთხოების მართვის სისტემა ასახავს კომპანიის ძირითად ღირებულებებს - პასუხისმგებლობას, გამჭვირვალობას და საქმიანობის ეფექტიანობას. იგი არა მხოლოდ აკმაყოფილებს მიმდინარე საქმიანობისთვის აუცილებელ უსაფრთხოების მოთხოვნებს, არამედ ქმნის საფუძველს სისტემის განვითარებისთვის, რეგულაციებთან და საერთაშორისო სტანდარტებთან შესაბამისობისთვის.

კიბერუსაფრთხოების ზომები

კიბერუსაფრთხოების ზომები წარმოადგენს შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“-ის ინფორმაციული უსაფრთხოების საერთო მიდგომის მნიშვნელოვან ნაწილს. მიზნად ისახავს პერსონალურ, საოპერაციო და ინფრასტრუქტურასთან დაკავშირებულ მონაცემებზე არასანქცირებული წვდომის, მათი არასწორი გამოყენების ან დაკარგვის თავიდან აცილებას.

კიბერუსაფრთხოების პროგრამა დანერგილია ინფორმაციული ტექნოლოგიების დამოუკიდებელ სპეციალისტთან თანამშრომლობით და მოიცავს ურთიერთდამხმარე დაცვის ღონისძიებებს, რომლებიც ითვალისწინებს როგორც ტექნიკურ, ისე ორგანიზაციულ რისკებს. აღნიშნული ღონისძიებები მიმართულია გავრცელებული საფრთხეების წინააღმდეგ, მათ შორის საზიანო პროგრამების, არასანქცირებული დისტანციური წვდომისა და შიდა რისკების შემცირების მიზნით.

კომპანიაში კიბერუსაფრთხოება უზრუნველყოფილია შემდეგი ზომებით:

- კომპიუტერული სისტემების დაცვა საზიანო პროგრამებისგან და დაცვის საშუალებების მუდმივი განახლება და კონტროლი ყველა მოწყობილობაზე. პროგრამები რეგულარულად ახლდება ცენტრალიზებულად და მოწმდება მესამე მხარის ინფორმაციული ტექნოლოგიების სპეციალისტების მიერ;
- ძლიერი პაროლების გამოყენება და სისტემაში შესვლისას დამატებითი დადასტურების მოთხოვნა დისტანციური წვდომისა და ადმინისტრაციული სისტემებისთვის. მომხმარებლის მონაცემები განისაზღვრება როლის მიხედვით და არ გამოიყენება სხვადასხვა სისტემაში ერთსა და იმავე ფორმით;
- მონაცემებზე წვდომის კონტროლი ისე, რომ თითოეულ თანამშრომელსა და კონტრაქტორს ჰქონდეს ინდივიდუალური მომხმარებლის ანგარიში. წვდომის უფლებები პერიოდულად გადაიხედება და საჭიროების შემთხვევაში იცვლება;
- სამუშაო მოწყობილობების დაცვა, მათ შორის პაროლების პერიოდული შეცვლა, ეკრანის ავტომატური დაბლოკვა, გარე მოწყობილობების გამოყენების შეზღუდვა და კომპიუტერულ პროგრამაში საეჭვო აქტივობის გამოვლენა
- სამუშაო სივრცეში დოკუმენტები და მობილური მოწყობილობები უნდა ინახებოდეს ისე, რომ მათზე წვდომა ჰქონდეთ მხოლოდ უფლებამოსილ პირებს;
- ჰიდროელექტროსადგურის მართვის სისტემების იზოლირება საჯარო ქსელებისგან;
- მონაცემთა სარეზერვო ასლების რეგულარული შექმნა და მათი უსაფრთხო შენახვა დისტანციურ გარემოში, ასევე აღდგენის შესაძლებლობის პერიოდული შემოწმება;
- უსაფრთხოების ზომების პერიოდული გადახედვა და შემოწმება ახალი საფრთხეების დროულად გამოსავლენად და აღმოსაფხვრელად;

კიბერუსაფრთხოება წარმოადგენს კომპანიის მართვის მნიშვნელოვან ნაწილს და არ შემოიფარგლება მხოლოდ ტექნიკური გადაწყვეტილებებით.

მონაცემთა დაცვა და სამართლებრივი მოთხოვნების შესრულება

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ სრულად ერთგულია პერსონალური და სენსიტიური ინფორმაციის დაცვის მიმართ, პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონისა და საერთაშორისო აღიარებული პრაქტიკის შესაბამისად.

კომპანია ამუშავებს პერსონალურ მონაცემებს არა მხოლოდ შიდა ადმინისტრაციული და დასაქმებასთან დაკავშირებული მიზნებისთვის, არამედ ობიექტზე დაშვების, კონტრაქტორების მართვის, სამართლებრივი მოთხოვნების შესრულებისა და დაინტერესებულ მხარეებთან ურთიერთობის ფარგლებში. შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ უზრუნველყოფს, რომ პერსონალური მონაცემები მუშავდებოდეს გამჭვირვალედ, სამართლიანად და მკაფიოდ განსაზღვრული მიზნებისთვის. მონაცემები არ გამოიყენება იმ მიზნებისთვის, რომლებიც წინასწარ არ არის განსაზღვრული.

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“-ში პერსონალურ მონაცემების დამუშავება ეფუძნება შემდეგ ძირითად პრინციპებს:

- გამოიყენება მხოლოდ ის პერსონალური მონაცემები, რაც აუცილებელია საქმიანობისთვის, მათ შორის ანაზღაურების, ობიექტზე დაშვების, ხელშეკრულებების მართვისა და ანგარიშგების მიზნით;
- პერსონალის, კონტრაქტორებისა და მესამე მხარის მონაცემები ინახება უსაფრთხოდ, როგორც ელექტრონულ, ისე ქაღალდზე არსებულ ფორმატში. მონაცემებზე წვდომა შეზღუდულია და განისაზღვრება პასუხისმგებლობის მიხედვით;
- თითოეულ პირს აქვს უფლება მიიღოს ინფორმაცია საკუთარი პერსონალური მონაცემების გამოყენების შესახებ, მოითხოვოს მათი გასწორება და კანონით დაშვებულ შემთხვევაში, წაშლა ან შეზღუდვა;
- პერსონალური მონაცემები ინახება მხოლოდ იმ ვადით, რაც აუცილებელია საქმიანობის ან კანონით განსაზღვრული მოთხოვნების შესასრულებლად. ამის შემდეგ მონაცემები იშლება, ან ინახება არქივში;
- მონაცემების ნადგურდება უსაფრთხო წესით, როგორც ელექტრონულ, ისე ქაღალდზე არსებულ ფორმატში. ქაღალდის დოკუმენტები ნადგურდება დაქუცმაცებით, ხოლო ელექტრონული მონაცემები იშლება შესაბამისი პროგრამების გამოყენებით;
- კონტრაქტორები და სხვა მესამე მხარეები, რომლებიც ამუშავებენ პერსონალურ მონაცემებს, მოქმედებენ ხელშეკრულებით განსაზღვრული მოთხოვნების შესაბამისად, რაც მოიცავს მონაცემების უსაფრთხო გამოყენებას და საჭიროების შემთხვევაში შემოწმების პროცესში თანამშრომლობას;
- თანამშრომლები და კონტრაქტორები რეგულარულად იღებენ ინფორმაციას მათ მონაცემებთან დაკავშირებული უფლებების შესახებ ტრენინგებისა და შიდა კომუნიკაციის საშუალებით;
- ვიდეომეთვალყურეობა გამოიყენება მხოლოდ უსაფრთხოების და სამართლებრივი მოთხოვნების შესრულების მიზნით. შესაბამისი ინფორმაცია წინასწარ არის მიწოდებული, ხოლო ჩანაწერები ინახება განსაზღვრული ვადით;
- მონაცემთა უსაფრთხოების დარღვევის შემთხვევაში მოქმედებს რეაგირების განსაზღვრული წესები, რაც მოიცავს ინციდენტის დაუყოვნებლივ შეტყობინებას, შემდგომ შეფასებას და საჭიროების შემთხვევაში შესაბამისი პირებისა და მარეგულირებელი ორგანოების ინფორმირებას. მიღებული ზომები აღირიცხება და კონტროლდება.

ტრენინგი და ცნობიერების ამაღლება

შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ განსაკუთრებულ ყურადღებას უთმობს თანამშრომლების ინფორმირებულობას ინფორმაციული უსაფრთხოების საკითხებზე. ყველა თანამშრომელი ვალდებულია გაიაროს შესაბამისი ტრენინგი ინფორმაციული უსაფრთხოების, კიბერუსაფრთხოების, პერსონალური მონაცემების დაცვისა და ინციდენტების შეტყობინების წესების შესახებ.

ტრენინგის მიზანია, თანამშრომლებმა გააცნობიერონ როგორც პრაქტიკული, ისე ეთიკური პასუხისმგებლობა სენსიტიურ ინფორმაციასთან მუშაობისა და ენერგეტიკული ინფრასტრუქტურის პირობებში საქმიანობის დროს. ახალი თანამშრომლები სისტემებზე წვდომის მიღებამდე ან ოპერირებიასთან დაკავშირებულ მონაცემებთან მუშაობის დაწყებამდე გადიან სავალდებულო შესავალ პროგრამას. ამ პროცესში ისინი ეცნობიან და ადასტურებენ კომპანიის შესაბამისობის პოლიტიკასა და ინფორმაციული უსაფრთხოების პოლიტიკას, რაც უზრუნველყოფს საერთო გაგებას უსაფრთხოების მოთხოვნების, ინფორმაციული სისტემების გამოყენების წესებისა და კანონით გათვალისწინებული ვალდებულებების შესახებ. ტრენინგები ტარდება ყოველწლიურად და საჭიროების შემთხვევაში ახლდება კანონმდებლობის ცვლილებების, უსაფრთხოების ინციდენტების, ან შიდა წესების გადახედვის საფუძველზე. ყველა ჩატარებული ტრენინგი აღირიცხება და ინახება შემდგომი შემოწმების მიზნებისთვის.

ამ პროგრამის საშუალებით შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ აძლიერებს ინდივიდუალურ პასუხისმგებლობას, ამცირებს ადამიანური შეცდომის რისკს და უზრუნველყოფს, რომ უსაფრთხოებისა და მონაცემთა დაცვის მოთხოვნები ერთგვაროვნად იყოს გაგებული და შესრულებული როგორც კომპანიის შიგნით, ისე პარტნიორებთან ურთიერთობაში.

ინფორმაციული უსაფრთხოების პოლიტიკის ყოველწლიური გადახედვის პროცესი

საერთაშორისო დონეზე აღიარებული გარემოსდაცვითი, სოციალური და მმართველობითი პრაქტიკების და სტანდარტების შესაბამისად, შპს „სი-სი-ი-ეიჩ ჰაიდრო VI“ ყოველწლიურად ახორციელებს ინფორმაციული უსაფრთხოების პოლიტიკის სრულმასშტაბიან გადახედვას წლის ბოლოს. ეს სისტემური გადახედვა, რომელსაც ხელმძღვანელობს კომპანიის გარემოსდაცვითი, სოციალური და მმართველობითი მენეჯერი, უზრუნველყოფს, რომ ჩვენი განცხადებები ზუსტად ასახავს მიმდინარე შეფასებებს, შესრულების მაჩვენებლებსა და ოპერირების პრაქტიკებს. თუ გადახედვის პროცესში განხორციელდება ცვლილებები, განახლებული დოკუმენტაცია გადის დეტალურ დამტკიცების პროცედურას. საწყის ეტაპზე, შემოთავაზებული ცვლილებები ყურადღებით განიხილება და მტკიცდება კომპანიის დირექტორის მიერ. შემდგომში, გადახედილი დოკუმენტი გადაეცემა კავკასიის განახლებადი ენერგიის ჰოლდინგის გარემოსდაცვითი, სოციალური, მმართველობითი და მდგრადობის ხელმძღვანელს საბოლოო დამტკიცებისათვის, რათა უზრუნველყოფილი იყოს, რომ თითოეული ცვლილება შეესაბამება ჩვენს ხარისხის, გამჭვირვალობისა და რეგულაციების შესაბამისობის ვალდებულებებს. დირექტორთა საბჭოს წევრები ინფორმირებულნი არიან ცვლილებების შესახებ, რაც აძლიერებს ჩვენს ერთგულებას მაღალი საერთაშორისო გარემოსდაცვითი, სოციალური და მმართველობითი სტანდარტების დაცვის მიმართ. განახლებული ვერსია იტვირთება კომპანიის ვებგვერდზე, ხოლო წინა ვერსია რჩება ხელმისაწვდომი საიტის არქივის საქაღალდეში.