ინფორმაციული უსაფრთხოების პოლიტიკა

ვერსია 2.0
სს “სილქნეტი”
2025

სარჩევი

1. ტერმინთა განმარტება

ინფორმაციული უსაფრთხოება - ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფა;

ინფორმაციული უსაფრთხოების პოლიტიკა – საქართველოს კანონის და სხვა ნორმატიული აქტების, საერთაშორისო სტანდარტების და სხვა შეთანხმებების გათვალისწინებით ჩამოყალიბებული ნორმებისა და პრინციპების ერთობლიობა, რომელიც ემსახურება სს სილქნეტის (შემდგომში - „სილქნეტი“, „კომპანია“ ან „ორგანიზაცია“) ინფორმაციული უსაფრთხოების უზრუნველყოფას;

ინფორმაცია - მონაცემთა ერთობლიობა, რომელთაც გააჩნია მიზანი და დანიშნულება. ინფორმაცია შესაძლოა არსებობდეს სხვადასხვა ფორმით: ქაღალდზე ნაბეჭდი ან ხელნაწერი, ის შესაძლოა ინახებოდეს ელექტრონული ფორმით, მისი გადაცემა შესაძლოა მოხდეს უშუალო მიწოდების გზით, ასლის/ელექტრონული ასლის გადაცემის, ფოსტით ან ელექტრონული საშუალებებით მიწოდების გზით, ვიდეო-მატარებლების მეშვეობით, საუბრის დროს ან სხვა საშუალებით;

ინფორმაციული სისტემა – ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას;

ინფორმაციული აქტივი (შემდგომში - „აქტივი“) - ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია სილქნეტისთვის;

ინფორმაციული აქტივის მფლობელი – პირი ან სტრუქტურული ერთეული, რომელსაც გააჩნია აქტივის შემუშავების, მართვის, კონტროლის, განვითარების, მხარდაჭერის და დაცვის დადასტურებული და რეგლამენტირებული უფლება და შესაბამისი პასუხისმგებლობა;

ინფორმაციული უსაფრთხოების რისკის მფლობელი - ინფორმაციულ აქტივებთან დაკავშირებული რისკების გამოვლენაზე, შეფასებაზე და მართვაზე პასუხისმგებელი და უფლებამოსილი პირი ან სტრუქტურული

ერთეული;

კონფიდენციალურობა - აქტივის მახასიათებელი, რომელიც გულისხმობს მის ხელმისაწვდომობას მხოლოდ ავტორიზებული პირებისთვის ან პროცესებისთვის, წინასწარ განსაზღვრული მოთხოვნის შესაბამისად;

მთლიანობა - აქტივის სიზუსტისა და სისრულის მახასიათებელი, უტყუარი ცოდნა იმისა, რომ ძირითადი მონაცემები და ინფორმაცია არის სწორი, არ არის შეცვლილი არაავტორიზებული პირების მიერ და ასახავს ზუსტ ფაქტებს;

ხელმისაწვდომობა - ავტორიზებული პირის მოთხოვნის შესაბამისად, წვდომისა და გამოყენებადობის მახასიათებელი, ანუ უტყუარი ცოდნა იმისა, რომ ინფორმაცია საჭირო დროს საჭირო ფორმით იქნება ხელმისაწვდომი ავტორიზებული პირებისთვის;

კონტროლი - ორგანიზაციული და/ან ტექნიკური ღონისძიებების ერთობლიობა, რომელიც ცვლის რისკის დონეს საფრთხის რეალიზაციის პრევენციის, მოწყვლადობის აღმოფხვრის ან ზეგავლენის მინიმიზაციის გზით;

საფრთხე – არასასურველი ინციდენტის პოტენციური მიზეზი;

ინფორმაციული უსაფრთხოების რისკი (შემდგომში „რისკი“) - შესაძლებლობა იმისა, რომ ინფორმაციული უსაფრთხოების საფრთხე ისარგებლებს ინფორმაციული უსაფრთხოების აქტივის ან აქტივების სისუსტით და ამგვარად მიაყენებს ზიანს ორგანიზაციას;

სისუსტე (მოწყვლადობა) – აქტივის ან კონტროლის სისუსტე, რომელიც შესაძლოა გამოყენებული იქნეს ერთი ან რამდენიმე საფრთხის მიერ;

ზეგავლენა – ზიანი (მაგალითად, ფინანსური ან რეპუტაციული), რომელიც შეიძლება მიადგეს ორგანიზაციას რისკის რეალიზების შემთხვევაში;

ინფორმაციის უსაფრთხოების ინციდენტი: არასასურველი ან მოულოდნელი ინფორმაციული უსაფრთხოების შემთხვევა ან შემთხვევების სერია, რომელსაც აქვს ბიზნეს ოპერაციების კომპრომეტირების და ინფორმაციული უსაფრთხოებისთვის საფრთხის შექმნის მნიშვნელოვანი შესაძლებლობა.

2. პოლიტიკის მიზანი და გავრცელების არეალი

ელექტრონული და მატერიალური ინფორმაცია, ისევე როგორც ამ ინფორმაციის დამუშავებაში მონაწილე პროცესები, ადამიანები, პროგრამული და აპარატურული უზრუნველყოფა, კორპორაციული ქსელი, **ინფორმაციული სისტემები** და მედია მოწყობილობები წარმოადგენენ ღირებულ **ინფორმაციულ აქტივებს** სილქნეტისთვის. შესაბამისად, აღნიშნული **ინფორმაციული აქტივების კონფიდენციალურობის, მთლიანობისა** და **ხელმისაწვდომობის** უზრუნველყოფა წარმოადგენს კომპანიის და მისი ხელმძღვანელობის სტრატეგიულ ამოცანას.

წინამდებარე პოლიტიკის მიზანია ჩამოაყალიბოს **ინფორმაციული უსაფრთხოების** მიმართ ერთიანი და თანმიმდევრული მართვის მიდგომები. ასევე, უზრუნველყოს ისეთი პროცესებისა და **კონტროლის** მექანიზმების ჩამოყალიბება, რაც, ერთის მხრივ, ხელს შეუწყობს **ინფორმაციული უსაფრთხოების რისკების** დროულ გამოვლენას და მართვას, ხოლო, მეორეს მხრივ, გააუმჯობესებს **ინფორმაციული აქტივების** დამუშავების პროცესების დაგეგმარების, აღსრულებისა და **კონტროლის** მიდგომებს.

წინამდებარე პოლიტიკა ვრცელდება სილქნეტის თანამშრომლებზე, დროებით დასაქმებულებზე, კონტრაქტორებსა და ყველა იმ პირზე, რომელსაც წვდომა აქვს კომპანიის **ინფორმაციულ აქტივებზე.** გარდა

ამისა, წინამდებარე პოლიტიკაში მოცემული **ინფორმაციული უსაფრთხოების** პრინციპები გათვალისწინებული უნდა იყოს კომპანიაში ყველა ახლად ინიცირებული პროცესის დაგეგმვისას.

პოლიტიკასთან შეუსაბამობა შეიძლება ჩაითვალოს ნდობის მნიშვნელოვან დარღვევად და შესაძლოა გამოიწვიოს პირის დისციპლინარული პასუხისმგებლობის საკითხის დაყენება, მათ შორის, შრომითი ურთიერთობის შეწყვეტა ან/და დამრღვევი პირისგან ზიანის ანაზღაურება.

წინამდებარე პოლიტიკა შესაბამისობაშია საქართველოს კანონთან „ინფორმაციული უსაფრთხოების შესახებ“ და ISO/IEC 27001:2013 უსაფრთხოების სტანდარტთან.

ორგანიზაცია, თავისი სპეციფიკიდან გამომდინარე, ამუშავებს დიდი რაოდენობით პერსონალურ მონაცემებს. სწორედ ამიტომ, ორგანიზაცია ვალდებულია სათანადოდ დაიცვას პერსონალური მონაცემების დამუშავების კანონიერება, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად.

3. ინფორმაციული უსაფრთხოების მიზნები და პრინციპები

სს „სილქნეტში“ **ინფორმაციული უსაფრთხოების** დანერგვა ემსახურება შემდეგი მიზნების უზრუნველყოფას:

- ინფორმაციული **აქტივების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის** დაცვა;
- **ინფორმაციული უსაფრთხოების რისკების** გამოვლენა და **რისკების** მოპყრობის გეგმების დანერგვის გზით მათ მისაღებ დონემდე შემცირება;
- თანამშრომლების, აბონენტების, მომწოდებლებისა და ბიზნეს პარტნიორების ინფორმაციის დაცვა
- საფრთხეების კუთხით არსებულ საკანონმდებლო, მარეგულირებელ და სახელშეკრულებო მოთხოვნებთან შესაბამისობა;
- ინფორმაციული უსაფრთხოების პოლიტიკების, პროცესებისა და დოკუმენტაციის მუდმივი გაუმჯობესება;
- თანამშრომლებში ინფორმაციული უსაფრთხოების მაღალი კულტურისა და ცნობიერების განვითარება.

წინამდებარე პოლიტიკა ეფუძნება **ინფორმაციული უსაფრთხოების** შემდეგ ძირითად პრინციპებს:

- **სილქნეტის მისიისა და სტრატეგიის მხარდაჭერა: ინფორმაციული უსაფრთხოების** კომპანიის საქმიანობის პროცესებში ინტეგრირების გზით **ინფორმაციული უსაფრთხოების** საფრთხეებით გამოწვეული **რისკების** მინიმიზაცია;
- **უსაფრთხოების პოზიტიური კულტურის განვითარება:** სილქნეტის საჭიროებებზე მორგებული **ინფორმაციული უსაფრთხოების კონტროლის** მექანიზმების უზრუნველყოფა. **ინფორმაციული უსაფრთხოების** უზრუნველყოფის პროცესში ინფორმაციული უსაფრთხოების სამსახურსა და სხვა სტრუქტურულ მიმართულებებს შორის ეფექტური ურთიერთთანამშრომლობის ჩამოყალიბება;
- **ხარისხისა და დამატებითი ღირებულების უზრუნველყოფა: ინფორმაციული უსაფრთხოების კონტროლის** მექანიზმების დანერგვაზე გაწეული ხარჯები პროპორციულია **ინფორმაციული უსაფრთხოების საფრთხეებით** გამოწვეული **რისკებისა** და მათი პოტენციური **ზეგავლენისა;**
- **უფლება-მოვალეობებისა და ანგარიშვალდებულებების მკაფიოდ განსაზღვრა: ინფორმაციული უსაფრთხოების** დაცვა და უზრუნველყოფა წარმოადგენს სილქნეტის თითოეული თანამშრომლის მოვალეობას. ამასთან, სილქნეტი უზრუნველყოფს ძირითადი უფლება-მოვალეობებისა ფორმალურად განსაზღვრას და შესაბამისი პირების საჭირო უფლებამოსილებით აღჭურვას;

- **რისკებზე დაფუძნებული მიდგომის გამოყენება:** თანმიმდევრული და რეგულარული პროცესის გამოყენებით **ინფორმაციული უსაფრთხოების რისკების** დროული გამოვლენა და მოპყრობის ოპტიმალური გეგმების საშუალებით მათ მისაღებ დონემდე მინიმიზაცია. გადაწყვეტილებების მიღების პროცესში **რისკების** შეფასების შედეგების ინტეგრირება;
- **მუდმივი გაუმჯობესების უზრუნველყოფა:** სილქნეტი ოპერირებს დინამიურ ბიზნეს და ტექნოლოგიურ გარემოში. **ინფორმაციული უსაფრთხოების რისკების** ლანდშაფტი მუდმივად იცვლება. შესაბამისად, არსებული ორგანიზაციულ-ტექნიკური **კონტროლის** მექანიზმების ეფექტურობის უზრუნველყოფის მიზნით **ინფორმაციული უსაფრთხოების მართვის** რეგულარული გადახედვა, განხილვა და გაუმჯობესება.

4. ინფორმაციული უსაფრთხოების მართვა

ინფორმაციული უსაფრთხოების პრინციპებისა და მიზნების ეფექტურად და ეფექტიანად აღსრულებისთვის სილქნეტში დანერგილია **ინფორმაციული უსაფრთხოების მართვის სისტემა (შემდგომში - „იუმს“)**. აღნიშნული სისტემა დაფუძნებულია მუდმივი გაუმჯობესების იტერაციულ მოდელზე და მიზნად ისახავს მუდმივად ცვალებადი ბიზნეს გარემოს, ორგანიზაციული კონტექსტისა და საფრთხეების ლანდშაფტის რეგულარულ შეფასებას და ეფექტურ ინტეგრირებას **ინფორმაციული უსაფრთხოების მართვის სისტემაში**. დამატებითი დეტალები **იუმს-ის** დაგეგმვის, ოპერირების, მონიტორინგისა და მუდმივი გაუმჯობესების შესახებ მოცემულია „ინფორმაციული უსაფრთხოების მართვის სისტემის პოლიტიკაში“.

იუმს-ის გავრცელების სფერო დადგენილია და დეტალურად არის აღწერილი „ინფორმაციული უსაფრთხოების კონტექსტი, მოთხოვნები და გავრცელების სფეროს” დოკუმენტში, რომელიც ითვალისწინებს კომპანიის შიდა და გარე ფაქტორებს, ძირითადი დაინტერესებული მხარეების (მაგ., აქციონერები, დირექტორები, თანამშრომლები, მარეგულირებლები, აბონენტები და ა. შ.) საჭიროებებსა და მოლოდინებს, ისევე როგორ დაკავშირებულ საკანონმდებლო, მარეგულირებელ და სახელშეკრულებო მოთხოვნებს.

ინფორმაციული უსაფრთხოების რისკების მართვა

ინფორმაციული უსაფრთხოების ეფექტურობა უპირველესყოვლისა დამოკიდებულია სილქნეტის უნარზე დროულად გამოავლინოს და შეაფასოს საკუთარ **ინფორმაციულ აქტივებთან** დაკავშირებული **რისკები** და დანერგოს მათ მისაღებ დონემდე შესამცირებლად საჭირო **კონტროლი**.

ინფორმაციული უსაფრთხოების რისკების გამოვლენა და მართვა ხდება, როგორც **რისკების** შეფასების რეგულარული პროცესის, ასევე, **იუმს-ის** შიდა და გარე აუდიტის, **ინფორმაციული უსაფრთხოების ინციდენტების** მართვისა და სხვა საოპერაციო აქტივობების ფარგლებში, როგორც ეს დეტალურად აღწერილია „ინფორმაციული უსაფრთხოების რისკების შეფასებისა და მოპყრობის პოლიტიკის“ დოკუმენტში.

გამოვლენილ **რისკებზე** მოპყრობის გეგმის განსაზღვრა, დადასტურება და განხორციელება წარმოადგენს **ინფორმაციული უსაფრთხოების რისკის მფლობელის** პასუხისმგებლობას. **რისკების** შეფასების ანგარიშები **რისკის** მოპყრობის შეთანხმებულ გეგმებთან ერთად შემდგომი განხილვისა და მონიტორინგის მიზნით ინფორმაციული უსაფრთხოების მენეჯერის მიერ წარედგინება **ინფორმაციული უსაფრთხოების საბჭოს**.

ინფორმაციული უსაფრთხოების ინციდენტების მართვა

სილქნეტის ტექნოლოგიური კომპლექსურობის ზრდა, მესამე პირებთან მჭიდრო ურთიერთკავშირი და ახალი საფრთხეების მუდმივი ევოლუცია მნიშვნელოვნად ზრდის **ინფორმაციული უსაფრთხოებასთან**

დაკავშირებული ინციდენტების ხდომილების ალბათობას. ამ მიზნით, სილქნეტში შემუშავებულია „**ინფორმაციული უსაფრთხოების ინციდენტების მართვის პროცედურა**“, რომელიც შესაბამისობაშია „**ინფორმაციული უსაფრთხოების შესახებ**“ საქართველოს კანონთან და სტანდარტებისა და ტექნოლოგიების ნაციონალური ინსტიტუტის (ე. წ. „NIST“) მიერ გამოქვეყნებულ ინციდენტებზე რეაგირების სახელმძღვანელოსთან (ე. წ. „Computer Security Incident Handling Guide“). პროცედურა აყალიბებს კომპანიის მასშტაბით **ინფორმაციული უსაფრთხოების ინციდენტებზე** რეაგირების ერთიან და თანმიმდევრულ მიდგომას.

5. პასუხისმგებლობები

სამეთვალყურეო საბჭო

პასუხისმგებელია **ინფორმაციული უსაფრთხოების** ზოგადი სტრატეგიისა და პოლიტიკის განსაზღვრაზე.

ინფორმაციული უსაფრთხოების საბჭო

ინფორმაციული უსაფრთხოების საბჭო დაკომპლექტებულია უმაღლესი ხელმძღვანელობის წარმომადგენლებით, ხოლო მისი თავმჯდომარეა სილქნეტის გენერალური დირექტორი. ინფორმაციული უსაფრთხოების საბჭოს მიზანია ხელი შეუწყოს და ზედამხედველობა გაუწიოს **ინფორმაციული უსაფრთხოების** მუდმივ გაუმჯობესებას. ამასთან, ინფორმაციული უსაფრთხოების საბჭოს შემადგენლობა იძლევა ინფორმაციული უსაფრთხოების საკითხების ფართოდ განხილვისა და კონსესუსზე დაფუძნებული, ინფორმირებული გადაწყვეტილებების მიღების შესაძლებლობას.

ინფორმაციული უსაფრთხოების მენეჯერი

ინფორმაციული უსაფრთხოების მენეჯერი კოორდინაციას უწევს კომპანიის მასშტაბით ინფორმაციული უსაფრთხოების მართვას. პასუხისმგებელია ინფორმაციული უსაფრთხოების თემატური პოლიტიკების, პროცედურების, ინსტრუქციებისა და წესების ჩამოყალიბებაზე, რეგულარულ გადახედვაზე და გაუმჯობესებაზე. უზრუნველყოფს ინფორმაციული უსაფრთხოების შესახებ სილქნეტის თანამშრომლებში ცნობიერების ამაღლებას.

ინფორმაციული აქტივის მფლობელი

ინფორმაციული აქტივის მფლობელი პასუხისმგებელია ინფორმაციული უსაფრთხოების მოთხოვნების პრაქტიკაში გატარებაზე, კერძოდ, ინფორმაციული აქტივის უსაფრთხოების უზრუნველყოფის მიზნით, კონტროლის მექანიზმის განსაზღვრაზე და მათი აღსრულების მონიტორინგზე.

თითოეული დირექტორი და სტრუქტურული ერთეულის ხელმძღვანელი

თითოეული დირექტორი და სტრუქტურული ერთეულის ხელმძღვანელი პასუხისმგებელია უზრუნველყოს წინამდებარე პოლიტიკით გათვალისწინებული პრინციპებისა და მოთხოვნების სათანადო ინტეგრირება შესაბამისი (საკუთარი) სტრუქტურული ერთეულის საქმიანობის პროცესებში.

სილქნეტის თითოეული თანამშრომელი, დროებითი დასაქმებული, კონტრაქტორი და მესამე პირი, რომელსაც წვდომა აქვს **სილქნეტის ინფორმაციულ აქტივებზე** ვალდებულია გაეცნოს და დაიცვას წინამდებარე პოლიტიკა. გარდა ამისა, მათი პასუხისმგებლობა ითვალისწინებს წინამდებარე პოლიტიკის ნებისმიერ დარღვევის შესახებ ინფორმაციული უსაფრთხოების მენეჯერის დაუყოვნებლივ ინფორმირებას.

6. დოკუმენტის განხილვა

წინამდებარე პოლიტიკის მფლობელია ინფორმაციული უსაფრთხოების მენეჯერი, რომელიც პასუხისმგებელია უზრუნველყოს დოკუმენტის სულ მცირე წელიწადში ერთხელ, ან ორგანიზაციული კონტექსტის მნიშვნელოვანი ცვლილების შემთხვევაში გადახედვა, საჭიროებისამებრ განახლება და **ინფორმაციული უსაფრთხოების საბჭოსთვის** განსახილველად წარდგენა. ინფორმაციული უსაფრთხოების საბჭოს მიერ განხილული და შეთანხმებული პოლიტიკა საბოლოოდ მტკიცდება სილქნეტის გენერალური დირექტორის მიერ.

7. მოთხოვნები და შეზღუდვები

ინფორმაციაზე საკუთრების უფლება

ნებისმიერი ინფორმაცია, რომელიც იქმნება, ინახება და მუშავდება, სილქნეტის საქმიანობის პროცესების ფარგლებში, წარმოადგენს სილქნეტის საკუთრებას. მათი დამუშავება ხდება ორგანიზაციის მასშტაბით დადგენილი პოლიტიკებისა და პროცედურების შესაბამისად, გარდა იმ შემთხვევებისა, როდესაც მსგავსი დამუშავება არ ეწინააღმდეგება მოქმედი კანონმდებლობის მოთხოვნებს.

წვდომების კონტროლი

ინფორმაციასა და ინფორმაციის დამუშავების საშუალებებზე წვდომა ნებადართულია მხოლოდ უფლებამოსილ/ავტორიზებულ პირთათვის „მინიმალური პრივილეგიების“ (ე. წ. „Least Privileges“) და „აუცილებელი ცოდნის“ (ე. წ. „Need to Know“) პრინციპების გათვალისწინებით და დაცულია ავთენტიფიკაციისა და ავტორიზაციის ეფექტური მექანიზმებით.

გარდა ამისა, წვდომის ლეგიტიმურობისა და სისწორის უზრუნველსაყოფად, **ინფორმაციული აქტივის მფლობელები** რეგულარულად ახდენენ საკუთარ აქტივებზე არსებული წვდომების გადახედვას და, საჭიროების შემთხვევაში, კორექტირებას.

აკრძალული პროგრამული უზრუნველყოფა

ბიზნეს საქმიანობისთვის დაშვებულია მხოლოდ სილქნეტის მიერ წინასწარ ავტორიზებული პროგრამული უზრუნველყოფის გამოყენება. დამატებითი კონტროლის მიზნით, სილქნეტს განსაზღვრული აქვს არასტანდარტული და აკრძალული პროგრამული უზრუნველყოფის სია და შესაბამისი მონიტორინგის მექანიზმების საშუალებით უზრუნველყოფს მათი გამოყენების დროულ გამოვლენას და აღკვეთას.

მონაცემების შენახვა და გადაცემა

აბონენტებთან, ბიზნეს პარტნიორებთან და საზოგადოებასთან მონაცემთა მიმოცვლის პროცესში არასანქცირებული გასაჯაროების რისკების მინიმიზაციის მიზნით, კომპანიის მასშტაბით გამოიყენება მხოლოდ წინასწარ ავტორიზებული უსაფრთხო შენახვის, გადაცემისა და კომუნიკაციის სხვადასხვა ტექნოლოგიური გადაწყვეტა.

მკაცრად აკრძალულია ტექნოლოგიური გადაწყვეტების გამოყენება, რომლებიც ოფიციალურად არ არის მოწოდებული ან ავტორიზებული სილქნეტის მიერ. სილქნეტის საჭიროებიდან გამომდინარე, გამონაკლის შემთხვევაში, კონკრეტული გადაწყვეტის გამოყენება წინასწარ თანხმდება თანამშრომლის უშუალო ხელმძღვანელთან და ინფორმაციული უსაფრთხოების საბჭოსთან.

თანამშრომელთა უფლებები

სილქნეტი აძლევს თანამშრომლებს უფლებას გამოიყენონ კორპორაციული ბიზნეს ტექნოლოგიები (მაგ: კომპანიაში არსებული ელექტრონული პლატფორმები) პირადი მიზნებისთვის იმ დათქმით, რომ ასეთი გამოყენება განხორციელდება პასუხისმგებლიანი მიდგომით და შესაბამისობაში იქნება მოქმედი კანონმდებლობის, რეგულაციებისა და სილქნეტის „დასაშვები გამოყენების პოლიტიკის“ მოთხოვნებთან. დამატებითი კონტროლის სახით, ბიზნეს ტექნოლოგიების პირადი მიზნებისთვის გამოყენება ექვემდებარება სილქნეტის მხრიდან მკაცრ მონიტორინგს.

პაროლების უსაფრთხოება

სილქნეტის კორპორაციულ რესურსებსა და ინფორმაციაზე წვდომა დაცულია ავთენტიფიკაციის ეფექტური მექანიზმებით. ავთენტიფიკაციის ფარგლებში გამოყენებული პაროლის მახასიათებლები რეგულირდება „პაროლების მართვის პოლიტიკით“ და შესაბამისობაშია ინდუსტრიის საუკეთესო პრაქტიკებთან. კრიტიკული სისტემებისთვის, სილქნეტი დამატებით იყენებს ორ-ფაქტორიანი ავთენტიფიკაციის მექანიზმს, რომელიც სტანდარტულ პაროლთან ერთად ითვალისწინებს სისტემის მომხმარებლის მხრიდან დამატებითი ელემენტის წარდგენას, როგორიცაა, მაგალითად, შემთხვევითობის პრინციპით გენერირებული ერთჯერადი პაროლი (ე. წ. „One-time Password (OTP)”).

ელექტრონული ფოსტის გამოყენება

სამსახურებრივი მიზნებისთვის კომპანიის მასშტაბით გამოიყენება მხოლოდ სილქნეტის კორპორაციული ელექტრონული ფოსტა. პერსონალური ელექტრონული ფოსტის გამოყენება შეზღუდულია და მკაცრად კონტროლდება.

გარდა ამისა, ცნობიერების ამაღლების რეგულარული ტრენინგების ფარგლებში, თანამშრომლები ღებულობენ ინფორმაციას ელექტრონული ფოსტის გამოყენებასთან დაკავშირებული გავრცელებული საფრთხეებისა და მათთან ეფექტურად გამკლავების სასარგებლო რჩევების / რეკომენდაციების შესახებ.

ინტერნეტის გამოყენება

ინტერნეტი წარმოადგენს სილქნეტის საქმიანობის ეფექტურად და ეფექტიანად წარმოების უმნიშვნელოვანეს რესურსს, რომელიც გამოყენებულ უნდა იქნას სილქნეტის ბიზნეს ინტერესების შესაბამისად. კომპანიის თანამშრომლების მიერ ინტერნეტის გამოყენება მკაცრად კონტროლდება უსაფრთხოების სხვადასხვა მექანიზმის გამოყენებით, რათა მინიმუმამდე იქნას დაყვანილი ინფორმაციის არასანქცირებული გასაჯაროება / მოპოვება.

ანტივირუსი და უსაფრთხოების განახლებები

სილქნეტის თანამშრომლების მოწყობილობები (მაგ., პერსონალური კომპიუტერები, ლეპტოპები, მობილურები), ისევე როგორც, სერვერული ინფრასტრუქტურა დაცულია ეფექტური ანტივირუსული პროგრამული უზრუნველყოფით. ავტორიზებულ პირებს შეზღუდული აქვთ საკუთარ მოწყობილობებზე ანტივირუსული პროგრამული უზრუნველყოფის წაშლის, დეაქტივაციის ან უსაფრთხოების აუცილებელი განახლებების შეფერხების შესაძლებლობა. ანტივირუსული პროგრამული უზრუნველყოფის მიერ დაფიქსირებული ნებისმიერი საეჭვო მოვლენა ან ფაილი, შემდგომი დროული რეაგირების მიზნით, დეტალურად ანალიზდება ინფორმაციული უსაფრთხოების სამსახურის მიერ.

ტექნიკური სისუსტეების მართვა

სილქნეტი რეგულარულად ახდენს კორპორაციული ქსელის, ინფორმაციული სისტემებისა და რესურსების ტექნიკური სისუსტეების სკანირებას. გამოვლენილ სისუსტეებზე დროული რეაგირების, მათ შორის, უსაფრთხოების განახლებების დაყენების კოორდინაცია წარმოადგენს ინფორმაციული უსაფრთხოების სამსახურის პასუხისმგებლობას.

8. გამონაკლისები

აღნიშნული პოლიტიკიდან ყველა გამონაკლისი უნდა დაამტკიცოს სილქნეტის ინფორმაციული უსაფრთხოების საბჭომ.