სს „სილქნეტი“

მიმწოდებლის უსაფრთხოების პოლიტიკა

2019 წ.

წინამდებარე მიმწოდებლების უსაფრთხოების პოლიტიკა (შემდგომში „პოლიტიკა“) აღწერს უსაფრთხოების მოთხოვნებს სს „სილქნეტის“ (შემდგომში „სილქნეტი“) მიმწოდებლებისთვის. კონკრეტულ შემთხვევებში შესაძლებელია სხვა დამატებითი უსაფრთხოების მოთხოვნების გამოყენება, თუ მოხდება მხარეებს შორის შეთანხმება.

წინამდებარე პოლიტიკის მოთხოვნები გამოიყენება ყველა იმ იურიდიული/ფიზიკური პირის მიმართ, რომლებიც "სილქნეტს" აწვდიან პროდუქციას ან/და უწევენ მომსახურებას, ასევე, რომლებსაც „სილქნეტი“ აწვდის პროდუქციას ან/და უწევს მომსახურებას. აღნიშნული პოლიტიკა მათ შორის ვრცელდება მიმწოდებლებისა და მათი ქვეკონტრაქტორების თანამშრომლებსა და კონსულტანტებზე, მიუხედავად იმისა, ისინი უვადოდ არიან დასაქმებული თუ დროებით, უშუალო დასაქმებულები არიან თუ არა ან მათზე უშუალო ხელმძღვანელობა ხორციელდება თუ არა.

წინამდებარე პოლიტიკის მიზნებისთვის „მიმწოდებელი“ განიმატება როგორც სს „სილქნეტის“ კონტრაგენტი ნებისმიერი მხარე, შესაბამისი ხელშეკრულების კონტექსტიდან გამომდინარე.

წინამდებარე პოლიტიკა წარმოადგენს სს „სილქნეტსა“ და ნებისმიერ იურიდიულ/ფიზიკურ პირს შორის გაფორმებული ხელშეკრულების განუყოფელ ნაწილს.

1 ტერმინთა განმარტება

1.1. **„სილქნეტის მონაცემები“** - მონაცემები ან სხვა ინფორმაცია, რომელსაც სილქნეტი ან მისი სახელით მოქმედი პირი ხელმისაწვდომს ხდის მიმწოდებლისათვის, მათ შორის პერსონალური მონაცემები, აგრეთვე მიმწოდებლის მიერ ამგვარი მონაცემების დამუშავების შედეგი;

1.2. **„ინფორმაციის დამუშავების საშუალებები“** - ინფორმაციის დამამუშავებელ ნებისმიერი სისტემა, მომსახურებები ან ინფრასტრუქტურა, ან ფიზიკური ადგილმდებარეობა, სადაც ზემოაღნიშნული ხორციელდება.

1.3. **„აღრიცხვა“** - ინფორმაციის ან მოვლენების დეტალების აღრიცხვა ორგანიზებულ აღრიცხვის სისტემაში, რომელიც, როგორც წესი, დალაგებულია იმ თანმიმდევრობით, რა თანმიმდევრობითაც ჰქონდა ადგილი ამ ინფორმაციას ან მოვლენებს.

1.4. **„პერსონალური მონაცემები“** - ყველა ინფორმაცია, რომელიც შესაბამისი მონაცემთა დაცვის კანონმდებლობით, მათ შორის ევროკავშირის მონაცემთა დაცვის დირექტივის (ევროპარლამენტის და ევროსაბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC პერსონალური მონაცემების დამუშავებისა და ამგვარი მონაცემების თავისუფალ გადაადგილებისას ფიზიკური პირების დაცვის თაობაზე), ელექტრონულ კომუნიკაციებში მონაცემთა დაცვის შესახებ დირექტივა (ევროპარლამენტის და ევროსაბჭოს 2002 წლის 12 ივლისის 2002/58/EC დირექტივა, რომელიც შეეხება პერსონალურ მონაცემთა დამუშავებასა და ელექტრონული კომუნიკაციების სექტორში მონაცემთა დაცვას) და ზოგადი მონაცემთა დაცვის რეგულაცია (ევროპარლამენტის და ევროსაბჭოს 2016 წლის 27 აპრილის 2016/679 რეგულაცია პერსონალური მონაცემების

დამუშავებისა და ამგვარი მონაცემების თავისუფალ გადაადგილებისას ფიზიკური პირების დაცვის თაობაზე და გამაუქმებელი დირექტივა 94/46/RC), ასევე ნებისმიერი დამატება, ცვლილება ან განახლება (ყოველივე ზემოაღნიშნული ერთად მოიხსენიება როგორც „ევროკავშირის კანონმდებლობა“), ასევე მოცემულ დროს მოქმედი ყველა სავალდებულო ადგილობრივი კანონმდებლობა, რომელიც ცნობს ევროკავშირისა და სხვა მონაცემთა დაცვის და უსაფრთხოების დირექტივებს, კანონებს, რეგულაციებსა და გადაწყვეტილებებს, რომელიც დაკავშირებულია პირის მაიდენტიფიცირებელ მონაცემებთან. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, სახელით, მისამართით, სოციალური ნომრით, სააბონენტო ნომრით, IP მისამართით, ლოკაციის მონაცემით, ონლაინ იდენტიფიკატორით, ტრაფიკის მონაცემით ან შეტყობინების შინაარსით, ან ერთი ან მეტი ფაქტორით, რომელიც უკავშირდება ფიზიკური პირის ფიზიკურ, ფსიქოლოგიურ, გენეტიკურ, მენტალურ, ეკონომიკურ, კულტურულ ან სოციალურ იდენტობას საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.

1.5. **„მომსახურებები“** - მიმწოდებლის ან მისი სახელით მოქმედი პირის (ხელშეკრულებით მხარეების მიერ შემდგომში განსაზღვრული) მიერ სილქნეტისთვის მიწოდებულ მომსახურებებს.

1.6. **„მიმწოდებლის პერსონალი“** - ნებისმიერ პირი, რომელიც მუშაობს მიმწოდებლის სახელით, როგორიცაა, მაგალითად თანამშრომლები, კონსულტანტები, კონტრაქტორები და ქვეკონტრაქტორი.

1.7. **„უსაფრთხოების კონტროლი“** - ტექნიკური კონტრღონისძიება, ან ორგანიზაციული მოწყობა ან პროცესი, რომელიც ხელს უწყობს IT სისტემების უსაფრთხოების ხარისხის შენარჩუნებას.

1.8. **„უსაფრთხოების ინციდენტები“** - ერთი ან რიგი არასასურველი ან მოულოდნელი უსაფრთხოების მოვლენები, რომლებიც მაღალი ალბათობით საფრთხის შემცველია ბიზნეს ოპერაციებისა და უსაფრთხოებისათვის.

1.9. **„მგრძნობიარე (სენსიტიური) პროდუქტები“** და **„მგრძნობიარე (სენსიტიური) მომსახურებები“** - ნებისმიერი პროდუქტი ან მომსახურება, რომელიც განსაზღვრულია, როგორც მგრძნობიარე (სენსიტიური) სილქნეტის მიერ. მგრძნობიარე (სენსიტიური) პროდუქტები ან მგრძნობიარე (სენსიტიური) მომსახურებები მკაფიოდ უნდა იყოს დოკუმენტირებული შესაბამის ხელშეკრულებაში.

1.10. „**ფსევდონიმიზაცია**“ - მონაცემთა იმგვარ დამუშავება, როდესაც შეუძლებელია პერსონალური მონაცემების დაკავშირება კონკრეტულ მონაცემთა სუბიექტთან დამატებითი ინფორმაციის გამოყენების გარეშე და გულისხმობს ასეთი დამატებითი ინფორმაციის შენახვას განცალკევებით და ტექნიკური და ორგანიზაციული ზომების მიღებას, რათა პერსონალური მონაცემი აღარ უკავშირდებოდეს იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.

2. მოქმედების ფარგლები

2.1. წინამდებარე პოლიტიკა მოქმედებს როდესაც:

2.1.1. მიმწოდებელი დაამუშავებს სილქნეტის მონაცემებს.

2.1.2. მიმწოდებელი შევა სილქნეტის შენობაში.

2.1.3. მიმწოდებელს ექნება წვდომა, მათ შორის დისტანციური წვდომა, სილქნეტის ქსელზე ან IT სისტემებზე.

2.1.4. მიმწოდებელი ეხება სილქნეტის ინფორმაციის დამამუშავებელ მოწყობილობას.

2.1.5. სილქნეტი მიიჩნევს მიმწოდებელს მგრძნობიარე (სენსიტიური) პროდუქტების და/ან მგრძნობიარე (სენსიტიური) მომსახურებების მიმწოდებლად და მიმწოდებელი იდენტიფიცირებულია ასეთად, შესაბამისი ხელშეკრულების თანახმად.

3. მიმწოდებლის ზოგადი პასუხისმგებლობა

3.1. მიმწოდებელი სრულად პასუხისმგებელია მიმწოდებლის პერსონალის მიერ წინამდებარე პოლიტიკის მოთხოვნების შესრულებაზე.

3.2. მიმწოდებელი ვალდებულია განახორციელოს ღონისძიებები, რომელიც უზრუნველყოფს წინამდებარე პოლიტიკის შესრულებას, სილქნეტისთვის ნებისმიერი დავალების შესრულების დაწყებამდე.

3.3. სილქნეტისგან მოთხოვნის მიღების შემთხვევაში, მიმწოდებელი ვალდებულია შეატყობინოს სილქნეტს, თუ როგორ ასრულებს წინამდებარე პოლიტიკის მოთხოვნებს და რა ზომები მიიღო მიმწოდებელმა აღნიშნული პოლიტიკის შესასრულებლად.

3.4. მიმწოდებელმა უნდა აცნობოს სილქნეტს უსაფრთხოების ნებისმიერი ინციდენტის თაობაზე (მათ შორის, და არა მხოლოდ პერსონალური მონაცემების დამუშავებასთან დაკავშირებულ ინციდენტებზე) რაც შეიძლება სწრაფად, მაგრამ არაუგვიანეს 24 საათისა უსაფრთხოების ინციდენტის იდენტიფიცირებიდან.

3.5. მიმწოდებელი უზრუნველყოფს, რომ სილქნეტის ნებისმიერი მონაცემების დამუშავება შესაბამისობაში იქნება წინამდებარე პოლიტიკასთან.

3.6. მიმწოდებელი დააბრუნებს ან გაანადგურებს (როგორც სილქნეტი განსაზღვრავს) სილქნეტის ნებისმიერ მონაცემებს და მათ ასლებს. ხელშეკრულების შეწყვეტისას ან სილქნეტის მიერ მოთხოვნისას, მიმწოდებელი წერილობით დაუდასტურებს სილქნეტს ზემოაღნიშნული მოთხოვნის შესრულებას.

3.7. მიმწოდებელი არ დაუშვებს სილქნეტის მონაცემებზე ნებისმიერი მხარის დაშვებას (აღნიშნული შესაძლოა აგრეთვე ეხებოდეს ახალ, გაფართოებულ, განახლებულ, გახანგრძლივებულ ან სხვაგვარად შეცვლილ რეალურ დროში ქსელზე წვდომას) სილქნეტის წინასწარი წერილობითი თანხმობის გარეშე.

4. უსაფრთხოების მოთხოვნები

4.1. რისკების მართვა

4.1.1. უსაფრთხოების რისკების მართვა

4.1.1.1. მიმწოდებელი ვალდებულია მოახდინოს ინფორმაციის კონფიდენციალურობასთან, მთლიანობასა და ხელმისაწვდომობასთან დაკავშირებული უსაფრთხოების რისკების იდენტიფიცირება და ამგვარი შეფასების საფუძველზე დანერგოს შესაბამისი ტექნიკური და ორგანიზაციული ზომები არსებული რისკის შესაბამისი უსაფრთხოების დონის უზრუნველსაყოფად.

4.1.1.2. მიმწოდებელი ვალდებულია ჰქონდეს დოკუმენტირებული პროცესები და პრაქტიკა თავის ოპერაციებში რისკებთან გასამკლავებლად.

4.1.1.3. მიმწოდებელი ვალდებულია პერიოდულად შეაფასოს რისკები, რომელიც უკავშირდება ინფორმაციულ სისტემებსა და დამუშავებას, ინფორმაციის შენახვასა და გადაცემას.

4.2. უსაფრთხოების რისკების მართვა

4.2.1. მიმწოდებელი ვალდებულია გამოავლინოს და შეაფასოს ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის შესახებ უსაფრთხოების რისკები და ამგვარი შეფასების საფუძველზე განახორციელოს შესაბამისი ტექნიკური და ორგანიზაციული ზომები, რათა უზრუნველყოს უსაფრთხოების დონე, რომელიც შეესაბამება კონკრეტული პერსონალური მონაცემთა ტიპებსა და მიმწოდებლის მიერ მისი დამუშავების მიზნებს, მათ შორის:

4.2.1.1. პერსონალური მონაცემების ფსევდონიმიზაცია და დაშიფვრა;

4.2.1.2. ინფორმაციის კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა, ასევე დამუშავების სისტემებისა და მომსახურების მოქნილობის მუდმივად უზრუნველყოფა;

4.2.1.3. ფიზიკური ან ტექნიკური ინციდენტის დროს სილქნეტის მონაცემებზე ხელმისაწვდომობის დროულად აღდგენის შესაძლებლობის უზრუნველყოფა;

4.2.1.4. პროცესის უსაფრთხოების უზრუნველმყოფი ტექნიკური და ორგანიზაციული საშუალებების რეგულარული შემოწმებისა და შეფასების პროცესის არსებობა.

4.2.2. მიმწოდებელს უნდა ჰქონდეს სილქნეტის მონაცემების დამუშავებისას არსებული რისკების მართვის დოკუმენტურად გაწერილი პროცედურები და პრაქტიკა.

4.2.3. მიმწოდებელი ვალდებულია პერიოდულად შეაფასოს პერსონალურ მონაცემებთან დაკავშირებულ საინფორმაციო სისტემებთან, დამუშავებასთან, შენახვასა და გადაცემასთან დაკავშირებული რისკები.

4.3. ინფორმაციული უსაფრთხოების პოლიტიკა

4.3.1. მიმწოდებელს უნდა ჰქონდეს განსაზღვრული და დოკუმენტირებული ინფორმაციული უსაფრთხოების მართვის სისტემა (ISMS), მათ შორის ინფორმაციული უსაფრთხოების პოლიტიკა და პროცედურები ადგილზე, რაც დამტკიცებული უნდა იყოს მიმწოდებლის ხელმძღვანელობის მიერ. აღნიშნული გამოქვეყნებული უნდა იყოს მიმწოდებლის ორგანიზაციაში და უნდა ეცნობოს მიმწოდებლის შესაბამის პერსონალს.

4.3.2. მიმწოდებელი ვალდებულია პერიოდულად გადახედოს უსაფრთხოების პოლიტიკასა და პროცედურებს და განაახლოს ისინი, თუ აღნიშნული საჭიროა უსაფრთხოების დირექტივებთან მათ შესაბამისობაში მოსაყვანად.

4.4. ინფორმაციული უსაფრთხოების ორგანიზება

4.4.1. მიმწოდებელი ვალდებულია ჰქონდეს განსაზღვრული და დოკუმენტირებული უსაფრთხოების როლები და პასუხისმგებლობები საკუთარ ორგანიზაციაში.

4.4.2. მიმწოდებელმა უნდა დანიშნოს სულ მცირე ერთი პირი, რომელსაც აქვს უსაფრთხოების სათანადო კომპეტენცია და რომელსაც დაეკისრება უსაფრთხოების დირექტივების თანახმად უსაფრთხოების ზომების განხორციელების ზოგადი პასუხისმგებლობა და რომელიც იქნება სილქნეტის უსაფრთხოების სამსახურის თანამშრომლებისათვის საკონტაქტო პირი.

4.5. ადამიანური რესურსების უსაფრთხოება

4.5.1. მიმწოდებელი ვალდებულია უზრუნველყოს, რომ მისი პერსონალი ინფორმაციას ეპყრობოდეს ხელშეკრულებით გათვალისწინებული კონფიდენციალურობის დონის შესაბამისად.

4.5.2. მიმწოდებელი ვალდებულია უზრუნველყოს, რომ მიმწოდებლის შესაბამისი პერსონალისათვის ცნობილია ხელშეკრულების ფარგლებში ინფორმაციის, ობიექტებისა და სისტემების შეთანხმებული გამოყენების თაობაზე (მათ შორის გამოყენების შეზღუდვებზეც). სილქნეტი უფლებამოსილია მოითხოვოს მიმწოდებლის თითოეული თანამშრომლისაგან ხელმოწერილი დოკუმენტი, რომელშიც აღნიშნულია, რომ მან გაიგო და შეასრულებს წინამდებარე პოლიტიკას და უზრუნველყოფს ინფორმაციის, სისტემებისა და ობიექტების შეთანხმებულ გამოყენებას.

4.5.3. მიმწოდებელი ვალდებულია უზრუნველყოს, რომ მიმწოდებლის ნებისმიერი სპეციალისტი, რომელიც ასრულებს ხელშეკრულებით გათვალისწინებულ დავალებებს, არის სანდო, აკმაყოფილებს და დავალების შესრულების მთელი პერიოდის განმავლობაში დააკმაყოფილებს უსაფრთხოების დადგენილ კრიტერიუმებს და დაექვემდებარა სათანადო შემოწმებას.

4.5.4. მიმწოდებელი, სანამ დანიშნავს პერსონალს სილქნეტის დავალების შესასრულებლად, ვალდებულია აცნობოს სილქნეტს და მიიღოს მისგან წერილობითი ნებართვა შემდეგ შემთხვევებში: (i) პირს სილქნეტთან ან შესაბამის დავალებებთან დაკავშირებით აქვს ინტერესთა კონფლიქტი, ან (ii) პასუხისგებაში იყო მიცემული სისხლის სამართლის ნებისმიერი სახის დანაშაულისათვის უკანასკნელი სამი (3) წლის განმავლობაში დავალების შესრულებამდე, i) თუ მიმწოდებლის პერსონალი ნებისმიერ დროს განახორციელებს სილქნეტის კლიენტებთან ან პერსონალთან დაკავშირებული პერსონალური მონაცემების დამუშავებას, ან სილქნეტის მომხმარებლისათვის ან თუ, ii) მიმწოდებლის პერსონალი ჩართულია ისეთი დავალებების შესრულებაში, რომელიც სილქნეტის მიერ კლასიფიცირებულია როგორც სენსიტიური. სილქნეტმა ხელშეკრულების გაფორმებისას ან მიმწოდებლის პერსონალის მიერ მომსახურების/დავალების განხორციელებამდე სულ მცირე 2 კვირით ადრე უნდა უზრუნველყოს იმ ინფორმაციის მიწოდება, რომლითაც დადგენილია თუ რა ამოცანები/დავალებები კლასიფიცირდება როგორც სენსიტიური.

4.5.5. მიმწოდებელი ვალდებულია უზრუნველყოს, რომ მიმწოდებლის პერსონალი, რომელსაც აქვს უსაფრთხოების პასუხისმგებლობები, არის სათანადოდ მომზადებული უსაფრთხოებასთან დაკავშირებული მოვალეობების შესასრულებლად.

4.5.6. მიმწოდებელი ვალდებულია შესაბამისი პერსონალისთვის უზრუნველყოს პერიოდული ცნობიერების ამაღლების ტრენინგები უსაფრთხოების დარგში. ამგვარი ტრენინგი უნდა მოიცავდეს, შეზღუდვის გარეშე შემდეგ ინფორმაციას:

4.5.6.1. როგორ უნდა უზრუნველყოს მომხმარებელთა ინფორმაციის უსაფრთხოება (კონფიდენციალურობის დაცვა, მთლიანობა და ინფორმაციის ხელმისაწვდომობა);

4.5.6.2. რატომ არის ინფორმაციული უსაფრთხოება საჭირო მომხმარებელთა ინფორმაციისა და სისტემების დასაცავად;

4.5.6.3. საფრთხის ტიპები (როგორიცაა პირადი მონაცემების მოპარვა, საზიანო პროგრამები, სისტემის გატეხვა, ინფორმაციის გაჟონვა და საფრთხე თანამშრომლების მხრიდან);

4.5.6.4. ინფორმაციული უსაფრთხოების პოლიტიკის შესრულებისა და დაკავშირებული სტანდარტების/პროცედურების გამოყენების მნიშვნელობა;

4.5.6.5. პერსონალური პასუხისმგებლობა ინფორმაციულ უსაფრთხოებაზე (როგორიცაა, მომხმარებელთა კონფიდენციალური ინფორმაციის დაცვა და ფაქტობრივ და საეჭვო უსაფრთხოების ინციდენტებზე შეტყობინება).

4.6. აქტივების მართვა

4.6.1. მიმწოდებელი ვალდებულია ჰქონდეს აქტივების მართვის განსაზღვრული და დოკუმენტირებული სისტემა, და აწარმოოს ყველა შესაბამისი აქტივისა და მათი მესაკუთრეების განახლებული აღრიცხვა. ინფორმაციული აქტივები მოიცავს (მაგრამ შეზღუდული არ არის) IT სისტემებს, სარეზერვო და/ან მოძრავ ინფორმაციის მატარებელს, რომელიც შეიცავს მგრძნობიარე (სენსიტიური) ინფორმაციას, დასაშვებობის უფლებებს, პროგრამულ უზრუნველყოფას და კონფიგურაციას.

4.6.2. მიმწოდებელი ვალდებულია დაადოს ნიშანი, დაამუშაოს და დაიცვას ინფორმაცია ინფორმაციის კლასიფიკაციის წინასწარ განსაზღვრული სისტემის მიხედვით, იმ დროისათვის მოქმედი უსაფრთხოების სტანდარტების შესაბამისად (მათ შორის მოძრავი ინფორმაციის მატარებლის შენახვა, განკარგვა და ფიზიკური გადაცემა).

4.6.3. მიმწოდებელი ვალდებულია გაატაროს ზომები, რომლებიც უზრუნველყოფს გადაცემულ, შენახულ ან დამუშავებულ მყიდველის მონაცემებს შემთხვევითი, არაავტორიზებული ან უკანონო დაკარგვის, განადგურების, შეცვლის ან დაზიანებისგან.

4.6.4. მიმწოდებელი ვალდებულია იქონიოს დამუშავებული სილქნეტის მონაცემების განახლებული სია. სია უნდა შეიცავდეს შემდეგ ინფორმაციას:

4.6.4.1. დამუშავებული მონაცემები;

4.6.4.2. შენახვის დეტალები, როგორიცაა აქტივების სახელი, ადგილმდებარეობა და ა.შ.

4.7. დასაშვებობის კონტროლი

4.7.1. მიმწოდებელი ვალდებულია ჰქონდეს წვდომის კონტროლის განსაზღვრული და დოკუმენტირებული პოლიტიკა ობიექტებზე, ადგილსამყოფელებზე, ქსელზე, სისტემაზე, აპლიკაციასა და ინფორმაციაზე/მონაცემებზე წვდომისათვის (მათ შორის ფიზიკური, ლოგიკური და დისტანციური წვდომის კონტროლი), ავტორიზებული

პროცესი მომხმარებლის წვდომასა და პრივილეგიებზე, წვდომის უფლების გაუქმების პროცედურები და მიმწოდებლის პერსონალისათვის წვდომის პრივილეგიების მისაღები გამოყენება.

4.7.2. მიმწოდებელი ვალდებულია ჰქონდეს მომხმარებლის რეგისტრაციისა და რეგისტრაციის გაუქმების ფორმალური და დოკუმენტირებული პროცესი, რაც საშუალებას მისცემს წვდომის უფლებების დადგენას.

4.7.3. მიმწოდებელმა უნდა მიანიჭოს წვდომის პრივილეგიები ცოდნის საჭიროებისა და მინიმალური პრივილეგიის პრინციპებზე დაყრდნობით.

4.7.4. მიმწოდებელი ვალდებულია გამოიყენოს ძლიერი ავტორიზაცია (რამდენიმე საფეხურიანი) დისტანციური წვდომის მომხმარებლებისა და იმ მომხმარებლებისათვის, რომლებიც არასანდო ქსელიდან ამყარებენ უკავშირდებიან.

4.7.5. მიმწოდებელი ვალდებულია უზრუნველყოს, რომ მიმწოდებლის პერსონალს ჰქონდეს პერსონალური და უნიკალური იდენტიფიკატორი (მომხმარებლის სახელი), და გამოიყენოს ავტორიზაციის სათანადო ტექნიკა, რომელიც ადასტურებს და უზრუნველყოფს მომხმარებელთა ვინაობას.

4.8. კრიპტოგრაფია

4.8.1. მიმწოდებელი ვალდებულია უზრუნველყოს კონფიდენციალურ და საიდუმლო ინფორმაციაზე (როგორიცაა პერსონალური მონაცემები) კრიპტოგრაფიის სათანადო და ეფექტიანი გამოყენება, სილქნეტის კონფიდენციალურობის კლასიფიკაციის სქემის თანახმად.

4.8.2. მიმწოდებელი ვალდებულია დაიცვას კრიპტოგრაფიული კოდები.

4.9. ფიზიკური და გარემოსდაცვითი უსაფრთხოება

4.9.1. მიმწოდებელი ვალდებულია დაიცვას ინფორმაციის გადამუშავების ობიექტები გარეგანი და ეკოლოგიური საფრთხეებისა და რისკებისაგან, მათ შორის დენის/საკაბელო უკმარისობისა და სხვა შეფერხებებისაგან, რაც გამოწვეულია მხარდამჭერი მოწყობილობების გაუმართაობით. აღნიშნული მოიცავს ფიზიკური პერიმეტრისა და მისასვლელის დაცვას.

4.9.2. მიმწოდებელი ვალდებულია სილქნეტის სახელით მიღებული ან გაგზავნილი საქონელი დაიცვას ქურდობისგან, მანიპულაციის ან განადგურებისგან.

4.9.3. სილქნეტის შენობებსა და სილქნეტის ოჯარით აღებულ შენობებში დაშვება

4.9.3.1. მიმწოდებლის დაშვება სილქნეტის შენობებსა და საკუთრებაში (როგორიცაა მონაცემთა ცენტრის შენობები, საოფისე შენობები, ტექნიკური ობიექტები) მოიცავს შემდეგს:

4.9.3.1.1. ხელშეკრულებით გათვალისწინებული დავალებების შესრულებისას, მიმწოდებელი ვალდებულია დაიცვას ის შიდა რეგულაციები, რაც დადგენილია სილქნეტის მიერ.

4.9.3.1.2. მიმწოდებლის პერსონალი ვალდებულია ატაროს პირადობის დამადასტურებელი მოწმობები ან სტუმრის სამკერდე ნიშნები, რომელიც უნდა იყოს შესამჩნევი სილქნეტის შენობაში მუშაობის განმავლობაში.

4.9.3.1.3. დავალების შესრულების შემდეგ, ან როდესაც მიმწოდებლის პერსონალი გადაერთვება სხვა დავალებებზე, მიმწოდებელი ვალდებულია დაუყოვნებლივ შეატყობინოს სილქნეტს ცვლილების თაობაზე და დააბრუნოს გასაღებები, ბარათები, სერტიფიკატები, სტუმრის სამკერდე ნიშნები და მსგავსი ნივთები.

4.9.3.1.4. გასაღებები და საბარათე გასაღებები პირადად უნდა იყოს ხელმოწერილი მიმწოდებლის პერსონალის მიერ და მათი გადაცემა უნდა მოხდეს მიღებისას განსაზღვრული წერილობითი წესების თანახმად. სილქნეტის გასაღების ან საბარათე გასაღების დაკარგვა დაუყოვნებლივ უნდა ეცნობოს სილქნეტს.

4.9.3.1.5. ნებართვის გარეშე სილქნეტის შენობაში ან შენობასთან ფოტოგადაღება აკრძალულია.

4.9.3.1.6. აკრძალულია სილქნეტის საქონლის სილქნეტის შენობიდან ნებართვის გარეშე გატანა.

4.9.3.1.7. მიმწოდებლის პერსონალი ვალდებულია არ დაუშვას არაუფლებამოსილი პირების შესვლა შენობაში.

4.10. ოპერაციული უსაფრთხოება

4.10.1. მიმწოდებელი ვალდებულია ჰქონდეს ცვლილებების მართვის დადგენილი სისტემა ბიზნეს პროცესებში, ინფორმაციის დამუშავების ობიექტებსა და სისტემებში ცვლილებების შესატანად. ცვლილებების მართვის სისტემა უნდა მოიცავდეს ტესტებსა და მიმოხილვებს ცვლილებების განხორციელებამდე, როგორიცაა გადაუდებელ ცვლილებებთან გამკლავების პროცედურები, წინა ვერსიაზე დაბრუნების პროცედურები წარუმატებელ ცვლილებებთან გასამკლავებლად, აღრიცხვა (log), რომელიც აჩვენებს, თუ რა იქნა შეცვლილი, როდის და ვის მიერ.

4.10.2. მიმწოდებელი ვალდებულია განახორციელოს ზიანის შემცველი პროგრამებისგან დაცვა, რათა უზრუნველყოს, რომ ნებისმიერი პროგრამული უზრუნველყოფა, რომელიც გამოყენებულია მიმწოდებლის მიერ სილქნეტისათვის საქონლის ან მომსახურების მისაწოდებლად, დაცული იყოს ზიანის შემცველი პროგრამებისაგან.

4.10.3. მიმწოდებელი ვალდებულია შექმნას კრიტიკული ინფორმაციის სარეზერვო ასლები (backup copies) და სატესტო სარეზერვო ასლები, რათა უზრუნველყოს, რომ შესაძლებელი იყოს ინფორმაციის აღდგენა სილქნეტთან შეთანხმების თანახმად.

4.10.4. მიმწოდებელი ვალდებულია აღრიცხოს და გააკონტროლოს მომხმარებლების ქმედებები, როგორიცაა დამუშავებული მონაცემების შექმნა, წაკითხვა, კოპირება, შეცვლა და წაშლა, ისევე როგორც გამონაკლისები, ხარვეზები და ინფორმაციული უსაფრთხოების მოვლენები და რეგულარულად გადახედოს ზემოაღნიშნულს. გარდა ამისა, მიმწოდებელი ვალდებულია დაიცვას და შეინახოს (სულ მცირე 6 თვის განმავლობაში) აღრიცხვის (log) ინფორმაცია და მოთხოვნის შემთხვევაში, სილქნეტს გადასცეს მონიტორინგის მონაცემები. დარღვევის დამადასტურებელი ანომალიების/ინციდენტების/ინდიკატორების შესახებ უნდა ეცნობოს 5.13 პუნქტში აღწერილი ინციდენტების მართვის მოთხოვნების თანახმად.

4.10.5. მიმწოდებელი ვალდებულია მართოს ყველა შესაბამისი ტექნოლოგიის, მაგალითად ოპერაციული სისტემების, მონაცემთა ბაზების, აპლიკაციების ხარვეზები პროაქტიულად და დროულად.

4.10.6. მიმწოდებელი ვალდებულია შექმნას უსაფრთხოების საწყისი მონაცემები ყველა შესაბამისი ტექნოლოგიისათვის, როგორიცაა ოპერაციული სისტემები, მონაცემთა ბაზები, აპლიკაციები.

4.10.7. მიმწოდებელი ვალდებულია უზრუნველყოს, რომ დეველოპმენტი განცალკევებული იყოს სატესტო და საწარმოო გარემოსაგან.

4.11. საკომუნიკაციო უსაფრთხოება

4.11.1. მიმწოდებელი ვალდებულია განახორციელოს ქსელის უსაფრთხოების კონტროლი, როგორიცაა მომსახურების დონე, ქსელის დაცვა (firewalling) და სეგრეგაცია ინფორმაციული სისტემების დასაცავად.

4.11.2. მიმწოდებელი ვალდებულია უზრუნველყოს, რომ კონფიდენციალური და საიდუმლო ხმოვანი კომუნიკაცია (უფრო დეტალურად ნაჩვენებია ქვემოთ) იყოს უსაფრთხო, რაც იმას ნიშნავს, რომ არ შეიძლება დაუშიფრავი კომუნიკაციის გამოყენება.

4.12. სისტემის შეძენა, განვითარება და შენარჩუნება (როდესაც პროგრამული უზრუნველყოფის დეველოპმენტს ან სისტემის დეველოპმენტს სილქნეტისთვის უზრუნველყოფს მიმწოდებელი)

4.12.1. მიმწოდებელი ვალდებულია განახორციელოს პროგრამული უზრუნველყოფისა და სისტემების დეველოპმენტის ციკლის წესები, მათ შორის ცვლილებისა და გადახედვის პროცედურების.

4.12.2. მიმწოდებელი ვალდებულია შეამოწმოს უსაფრთხოების ფუნქციონალურობა კონტროლირებად გარემოში დეველოპმენტის დროს.

4.13. მიმწოდებლების ურთიერთობა ქვე-კონტრაქტორებთან

4.13.1. მიმწოდებელი ვალდებულია წინამდებარე პოლიტიკა ასახოს იმ ქვე-კონტრაქტორებთან ხელშეკრულებებში, რომლებიც ასრულებენ ხელშეკრულებით გათვალისწინებულ დავალებებს.

4.13.2. მიმწოდებელი ვალდებულია რეგულარულად აკონტროლოს, გადასინჯოს და შეამოწმოს ქვე-კონტრაქტორების მიერ წინამდებარე პოლიტიკის შესრულება.

4.13.3. სილქნეტისგან მოთხოვნის შემთხვევაში, მიმწოდებელი ვალდებულია მიაწოდოს სილქნეტს ქვე-კონტრაქტორის მიერ უსაფრთხოების დირექტივების შესრულების მტკიცებულებები.

4.14. უსაფრთხოების ინციდენტების მართვა

4.14.1. მიმწოდებელი ვალდებულია ჰქონდეს უსაფრთხოების ინციდენტების მართვის დადგენილი პროცედურები.

4.14.2. მიმწოდებელი ვალდებულია სილქნეტს აცნობოს უსაფრთხოებასთან დაკავშირებული ინციდენტების, მათ შორის პერსონალურ მონაცემთა

დამუშავებასთან დაკავშირებული ინციდენტების თაობაზე დაუყოვნებლივ, მაგრამ არა უგვიანეს უსაფრთხოების ინციდენტის იდენტიფიცირებიდან 24 საათისა.

4.14.3. ყველა ცნობა უსაფრთხოების ინციდენტის შესახებ განიხილება როგორც კონფიდენციალური ინფორმაცია და დაშიფრული უნდა იყოს შესაბამისი ინდუსტრიული სტანდარტის მეთოდების გამოყენებით, როგორიცაა PGP;

4.14.4. უსაფრთხოების ინციდენტის ანგარიში უნდა შეიცავდეს სულ მცირე შემდეგ ინფორმაციას:

4.14.4.1. დაუყოვნებლივ შეტყობინების საჭიროების მიუხედავად, მიმწოდებელი ვალდებულია სილქნეტს წარუდგინოს წინასწარი წერილობითი წინასწარი ანგარიში ნებისმიერი იმ უსაფრთხოების ინციდენტის თაობაზე, რომელმაც შესაძლოა გავლენა იქონიოს სილქნეტზე ან სილქნეტის აქტივებზე ნებისმიერი სახით;

4.14.4.2. მოვლენების, მათ შორის, ინციდენტის შედეგების აღმოფხვრის მიზნით განხორციელებული ქმედებების თანმიმდევრობა;

4.14.4.3. ინფრასტრუქტურის, სისტემებისა და ინფორმაციის დაზიანებული ნაწილი;

4.14.4.4. მოსალოდნელი (ან გაურკვევლობის მაღალი დონის შემთხვევაში, ყველაზე უარესი) შედეგები / ზემოქმედება;

4.14.4.5. უკვე განხორციელებული შედეგების აღმოსაფხვრელი ღონისძიებები;

4.14.4.6. უკვე განხორციელებული რისკის შემცირების ღონისძიებები;

4.14.4.7. შედეგების აღმოსაფხვრელად განსახორციელებელი ღონისძიებები , მათ შორის გეგმა (თარიღი; პასუხისმგებელი; დამოკიდებული);

4.14.4.8. რისკის შესამცირებლად განსახორციელებელი ღონისძიებები, მათ შორის გეგმა (თარიღი; პასუხისმგებელი; დამოკიდებული);

4.14.4.9. გამოცდილება შეჯამება;

4.14.5. მიმწოდებელი ვალდებულია უზრუნველყოს სილქნეტის დახმარება სასამართლო გამოძიების შემთხვევაში.

4.15. ბიზნესის უწყვეტობის მართვა

4.15.1. მიმწოდებელი ვალდებულია მოახდინოს ბიზნესის უწყვეტობის რისკების იდენტიფიცირება და მიიღოს აუცილებელი ზომები მსგავსი რისკების საკონტროლებლად და შესამსუბუქებლად.

4.15.2. მიმწოდებელი ვალდებულია ჰქონდეს დოკუმენტირებული პროცესები და პრაქტიკა ბიზნესის უწყვეტობის სამართავად.

4.15.3. მიმწოდებელმა უნდა უზრუნველყოს საინფორმაციო უსაფრთხოების ჩართვა ბიზნეს უწყვეტობის გეგმებში.

4.15.4. მიმწოდებელი ვალდებულია პერიოდულად შეაფასოს მისი ბიზნესის უწყვეტობის მართვის ეფექტიანობა და შესაბამისობა ხელმისაწვდომობის მოთხოვნებთან (ასეთის არსებობის შემთხვევაში).

4.16. შესაბამისობა

4.16.1. მიმწოდებელი ვალდებულია დაიცვას ყველა შესაბამისი საკანონმდებლო და სახელშეკრულებო მოთხოვნები, მათ შორის პერსონალურ მონაცემთა დაცვის თაობაზე.

4.16.2. მოთხოვნის შემთხვევაში, მიმწოდებელი ვალდებულია გაუმართლებელი დაყოვნების გარეშე მიაწოდოს სილქნეტს შესაბამისობის სტატუსის ანგარიში წინამდებარე პოლიტიკასთან დაკავშირებით.

4.16.3. სილქნეტი უფლებამოსილია შეამოწმოს, თუ როგორ ასრულებენ მიმწოდებელი ან ქვე-კონტრაქტორი უსაფრთხოების დირექტივებს ან შესაბამის მოთხოვნებს.