დანართი N1

# დისტანციური მუშაობა და ინფორმაციული უსაფრთხოება

არსებობს რამდენიმე ღონისძიება, რომლის განხორციელებაც ორგანიზაციებს შეუძლიათ საკუთარი აქტივებისა და რესურსების დასაცავად. უპირველეს ყოვლისა, საჭიროა დისტანციურ მუშაობასთან დაკავშირებული ყველა შესაძლო საფრთხისა და სარისკო არეების მკაფიო იდენტიფიცირება (ასევე, დოკუმენტირებაც). ეს დაეხმარება ორგანიზაციას უკვე გამოვლენილ რისკებზე სტრუქტურირებულ და მყისიერ რეაგირებაში და შესაბამისი ზომების მომზადებაში. ზოგიერთი ტიპური ღონისძიება, რომლის განხორციელებაც შესაძლებელია, ჩამოთვლილია ქვემოთ.

***უსაფრთხოებისა და კონფიდენციალურობის პოლიტიკა***

უნდა განისაზღვროს სათანადო ჩარჩო/დებულება/პოლიტიკა და მასთან დაკავშირებული პროცედურები, რაც, მათი უსაფრთხოების დონის გათვალისწინებით, მკაფიოდ ჩამოაყალიბებს არსებული აქტივებისა და რესურსების დისტანციური გამოყენების შესაძლებლობას. ნახსენებ პროცედურებში - მისაღები გამოყენების წესებში - ნათლად უნდა იყოს ნახსენები, თუ რა ქმედებების შესრულება შეიძლება, ან არ შეიძლება დისტანციურად მომუშავე თანამშრომლის მიერ კომპანიის აქტივების (ინფორმაციული სისტემების) მიმართ.

გარდა ამისა, სრულყოფილი უსაფრთხოების პოლიტიკის განხორციელება შეუძლებელია იმ საკითხების გათვალისწინების გარეშე, რომელთა ჩამონათვალი მოყვანილია „მოწყობილობები და მათი შიგთავსი“ ნაწილში.

***ტრენინგები და ცნობიერების ამაღლების პროგრამები***

ორგანიზაციის აქტივების უსაფრთხოების უზრუნველყოფის ერთ-ერთი ყველაზე ეფექტური გზა არის რეგულარული ტრენინგებისა და ცნობიერების ამაღლების კამპანიების განხორციელება. ღონისძიებების ფარგლებში ახსნილი უნდა იყოს რისკი, რომელიც დაკავშირებულია თანამშრომლების მიერ ინფორმაციული სისტემით სარგებლობის დროს (მაგ.: გაჟონვით) გამოწვეულ ზიანთან ორგანიზაციის, მისი მომხმარებლებისა და პერსონალისთვის. ცნობიერების ამაღლების ფარგლებში უნდა განიხილებოდეს აქტივების დაცვასთან დაკავშირებული ყველა თემა, დაწყებული საშინაო შემთხვევების თავიდან აცილებით (მაგ.: ოჯახის წევრების მიერ გამოწვეული, განსაკუთრებით მცირეწლოვანი), დამთავრებული უცნობი USB ბარათების მიერთებით ორგანიზაციის ლეპტოპში, ან უცხო მოწყობილობების გამოყენებით ორგანიზაციის სისტემებში შესასვლელად. ცნობიერების ამაღლების პროგრამებში ასევე აღსანიშნავია ერთ-ერთი თანამედროვე გავრცელებული საფრთხე - ფიშინგიც.

გარდა ამისა, ორგანიზაციული აქტივების უსაფრთხოების ზომების განსაზღვრასა და მონიტორინგში თანამშრომლების აქტიური ჩართვა მათ მფლობელობისა და მონაწილეობის უკეთეს შეგრძნებას აძლევს და ზრდის უსაფრთხოების პოლიტიკის დაცვის ხარისხს. ასევე,

დისტანციურად მომუშავე თანამშრომლები მუდმივად უნდა აცნობიერებდნენ, რომ მათი პირადი უსაფრთხოება პირდაპირ არის დამოკიდებული ორგანიზაციული აქტივების უსაფრთხოებაზე და მათ ყველაფერი უნდა იღონონ იმისთვის, რომ არ ჩაიგდონ საფრთხეში თავი.

საბოლოო ჯამში, თანამშრომლები ვალდებულნი არიან შეასრულონ ინფორმაციული უსაფრთხოების წესები, წინააღმდეგ შემთხვევაში მრავალი სხვა კონტროლის მექანიზმი შესაძლოა უსარგებლო აღმოჩნდეს.

### *უსაფრთხო დისტანციური კავშირი*

დისტანციურად მუშაობისას უსაფრთხო დისტანციური კავშირი ნამდვილად არის ერთ–ერთი საკვანძო საკითხი. ამ შემთხვევაში, ორგანიზაციის სისტემებზე წვდომა ხდება არამხოლოდ ოფისებიდან, არამედ უცნობი ადგილსამყოფელებიდან, რომელთაც აქვთ საკუთარი უნიკალური რისკი და სისუსტეები. კომპანიის სისტემებში შეჭრის რისკის თავიდან ასაცილებლად, ან აღნიშნული რისკის მინიმუმამდე დაყვანის მიზნით, უნდა განხორციელდეს ქსელური მონიტორინგი ორგანიზაციისთვის ხელმისაწვდომი ყველაზე თანამედროვე ტექნოლოგიური საშუალებების გამოყენებით.

გარდა ამისა, რეკომენდებულია კრიტიკული კომუნიკაცია დისტანციურად მომუშავე მოწყობილობებსა და კომპანიის სერვერებს შორის იყოს დაშიფრული (მაგალითად, VPN კავშირი). თავიდან უნდა იყოს აცილებული საჯარო Wi-Fi ქსელის გამოყენება.

### *მოწყობილობები და მათი შეგთავსი*

მოწყობილობის დაკარგვის შემთხვევაში, ბოროტმოქმედებს მარტივად შეუძლიათ წვდომის მოპოვება, თუ მოწყობილობა სათანადოდ არ იქნება უზრუნველყოფილი უსაფრთხოების ზომებით. ამიტომ, აუცილებელია კრიტიკული მონაცემების დაშიფვრა და ძლიერი (რთულად ამოსაცნობი) პაროლის გამოყენება. უნდა ხდებოდეს ეკრანის დაბლოკვა უმოქმედობის გარკვეული პერიოდის შემდეგ. ანტივირუსული პროგრამები რეგულარულად უნდა განახლდეს "იძულების" მეთოდის გამოყენებით, ხოლო მოწყობილობებს, რომელთა ანტივირუსული პროგრამა არ განახლებულა, უნდა შეეზღუდოთ დისტანციურად კრიტიკულ სისტემებთან დაკავშირების შესაძლებლობა.

ფიზიკური თვალსაზრისით, თანამშრომლებს შესაძლოა მიეცეთ კომპიუტერის საკეტები (მაგ.: ე.წ. კენსინგტონის საკეტები), რათა მათ შეძლონ კომპიუტერების ფიზიკურად ჩაკეტვა, როდესაც მისგან შორს იმყოფებიან.

ორგანიზაციის ხელმძღვანელობამ უნდა განიხილოს და გადაწყვეტილება მიიღოს შემდეგ საკითხებთან დაკავშირებით:

1. აქტივების სათანადო გამოყენების წესები;
2. დისტანციური მუშაობის როლები და პასუხისმგებლობები;
3. ინფორმაციული უსაფრთხოების შესახებ ცნობიერების ამაღლება, სწავლება და ტრენინგი;

4. დისციპლინა და დისციპლინარული ზომები;
5. მოწყობილობათა განლაგება და დაცვა;
6. მავნე კოდის საწინააღმდეგო კონტროლის მექანიზმები - ანტივირუსები, პერსონალური „ფაერვოლები“ და ა.შ.
7. მომხმარებელთა პაროლების მართვა - რთულად ამოცნობადი პაროლების გამოყენება;
8. მომხმარებელთა უფლებების მართვა - საუკეთესო პრაქტიკის მიხედვით, უფლებები შეზღუდული უნდა იყოს მხოლოდ აუცილებელი და ფუნქციის შესრულებისთვის საჭირო ინფორმაციით;
9. ინფორმაციის სარეზერვო ასლები;
10. ქსელის კონტროლის მექანიზმები;
11. გადაადგილებადი მედია-მატარებლების მართვა, მათ შორის - USB ბარათები;
12. ინფორმაციის გაცვლის პროცედურები ორგანიზაციის შიგნით თუ გარეთ;
13. ელექტრონული მიმოწერა;
14. წვდომის კონტროლის პოლიტიკა;
15. უყურადღებოდ დატოვებული მოწყობილობები;
16. გარე კავშირისთვის მომხმარებელთა ავთენტიფიკაცია;
17. სისტემაში დაცული შესვლის პროცედურები;
18. სესიის ვადის ამოწურვა, დაკავშირების ვადის შეზღუდვა’
19. მონაცემთა დაცვა და პირადი ინფორმაციის საიდუმლოება.

რასაკვირველია, ჩამოთვლილი საკითხები არ წარმოადგენს საჭირო ქმედებათა სრულ ჩამონათვალს, თუმცა დაეხმარება ორგანიზაციას უსაფრთხოების გარკვეული დონის უზრუნველყოფაში. ამ და სხვა საკითხების შესახებ გადაწყვეტილების მიღებით, ორგანიზაციას შეუძლია დისტანციურ მუშაობასთან დაკავშირებული რისკების შემცირება.

სრული ინფორმაცია შეგიძლიათ იხილოთ საქართველოს კანონში „ინფორმაციული უსაფრთხოების შესახებ“.