ბ რ ძ ა ნ ე ბ ა

N 149
21/10/2022

149-22-4-202210210052

საქართველოს სახალხო დამცველის აპარატის ინფორმაციული სისტემებისა და ინფორმაციული აქტივების პოლიტიკის დამტკიცების შესახებ

საქართველოს სახალხო დამცველის აპარატის ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, „საქართველოს სახალხო დამცველის შესახებ“ ორგანული კანონის 26-ე მუხლის პირველი პუნქტის საფუძველზე,

ვ ბ რ ძ ა ნ ე ბ:

1. დამტკიცდეს „საქართველოს სახალხო დამცველის აპარატის ინფორმაციული სისტემებისა და ინფორმაციული აქტივების პოლიტიკა“ თანდართული სახით (დანართი N1).
2. საქართველოს სახალხო დამცველის აპარატის თანამშრომლებს დაევალოს ინფორმაციული სისტემებისა და ინფორმაციული აქტივების პოლიტიკის 1.3 პუნქტის შესაბამისად სსიპ „ციფრული მმართველობის სააგენტოს“ ორგანიზებული „კიბერუსაფრთხოების საბაზისო კურსის“ გავლა და შესაბამისი სერთიფიკატის წარდგენა საქართველოს სახალხო დამცველის აპარატის სამართლებრივი უზრუნველყოფისა და ადამიანური რესურსების მართვის დეპარტამენტისათვის 2022 წლის 31 დეკემბრამდე.
3. ბრძანების გაცნობა დაინტერესებული პირებისათვის დაევალოს სამართლებრივი უზრუნველყოფისა და ადამიანური რესურსების მართვის დეპარტამენტს.
4. ბრძანება ძალაში შედის ხელმოწერისთანავე.
5. ბრძანება შეიძლება გასაჩივრდეს თბილისის საქალაქო სასამართლოს ადმინისტრაციულ საქმეთა კოლეგიაში (თბილისი, დავით აღმაშენებლის ხეივანი, მე–12 კმ, N64), მისი გაცნობიდან ერთი თვის ვადაში.

ნინო ლომჯარია

სახალხო დამცველი

დანართი N1

საქართველოს სახალხო დამცველის აპარატის ინფორმაციული სისტემებისა და ინფორმაციული აქტივების პოლიტიკა

2022 წელი

აპარატის ინფორმაციული სისტემებისა და ინფორმაციული აქტივების პოლიტიკა

სარჩევი

1. მიზანი

1.1. წინამდებარე წესები განსაზღვრავს საქართველოს სახალხო დამცველის აპარატში (შემდგომში აპარატი) ინფორმაციული სისტემების, აქტივების გამოყენების წესებს, ინფორმაციის კლასიფიკაციას, მასზე წვდომას, კონტროლს და ინფორმაციული უსაფრთხოების მართვის ძირითად მიმართულებებს და პრინციპებს.

1.2. წინამდებარე წესები წარმოადგენს საქართველოს სახალხო დამცველის აპარატის შინაგანაწესის ნაწილს შესასრულებლად სავალდებულოა აპარატში დასაქმებული ნებისმიერი პირისათვის.

1.3. წინამდებარე წესების შესრულების მიზნებისათვის, სახალხო დამცველის ყველა თანამშრომელი, ვისაც უწევს აპარატის ინფორმაციულ სისტემებთან მუშაობა ვალდებულია გაიაროს სსიპ „ციფრული მმართველობის სააგენტოს“ ორგანიზებული „კიბერუსაფრთხოების საბაზისო კურსი“ და შესაბამისი სერთიფიკატი წარუდგინოს აპარატის ადამიანური რესურსების მართვის ერთეულს. აპარატს ახალი თანამშრომელი აღნიშნულ სერთიფიკატს წარუდგენს შრომით სამართლებრივი ურთიერთობის წარმოშობიდან 1 თვის ვადაში.

1.4. თითოეული თანამშრომელი ვალდებულია შესაბამისი მიზნებისათვის გამოიყენოს Microsoft Office 365 - ის ფარგლებში აპარატის მიერ შეძენილი პროგრამები, მათ შორის online დისტანციური შიდა და გარე შეხვედრებისთვის Microsoft Teams.

2. წესის შემუშავების საფუძვლები

წინამდებარე წესები ემყარება შემდეგ სტანდარტებს:

- ISO/IEC 27001 სტანდარტი, მუხლები A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.3.1, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.3 A.9.4.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2

3. ძირითადი ტერმინები

- **კონფიდენციალურობის დონე** – ინფორმაციის მახასიათებელი, რომელიც განსაზღვრავს ინფორმაციის ხელმისაწვდომობას მხოლოდ უფლებამოსილი პირებისა და სისტემებისთვის.
- **მთლიანობა** – ინფორმაციის სიზუსტისა და სისრულის მახასიათებელი, როდესაც მისი შეცვლა შესაძლებელია მხოლოდ უფლებამოსილი პირებისა და სისტემების მიერ დაშვებული გზებით.
- **ხელმისაწვდომობის დონე** – მახასიათებელი, რომელიც განსაზღვრავს უფლებამოსილი პირების მიერ მის ხელმისაწვდომობას საჭიროების შემთხვევაში.
- **ინფორმაციული უსაფრთხოება** – წესების და ღონისძიებების ერთობლიობა, რომელიც უზრუნველყოფს ინფორმაციის კონფიდენციალურობას, მთლიანობასა და ხელმისაწვდომობის უზრუნველყოფას. ასეთი ღონისძიებები შეიძლება იყოს პროცესები და ინსტრუმენტები, რომლებიც შემუშავებულია ინფორმაციის მოდიფიკაციის, შეფერხების, განადგურებისა და შემოწმებისგან დასაცავად.
- **ინფორმაციული უსაფრთხოების მართვის სისტემა** – მართვის პროცესის ნაწილი, რომელიც უზრუნველყოფს ინფორმაციული უსაფრთხოების დაგეგმვას, დანერგვას, მხარდაჭერას, მონიტორინგსა და მის გაუმჯობესებას.
- **პერსონალური და განსაკუთრებული კატეგორიის მონაცემი** - „პერსონალურ მონაცემთა დაცვის“ შესახებ საქართველოს კანონით განსაზღვრული მონაცემები.

- **IT უსაფრთხოების მონაცემები** - შეიძლება მოიცავდეს მომხმარებლის Username-ებს და პაროლების სიებს, დაშიფვრის გასაღებებს (Keypads), ქსელის სტრუქტურასა და სხვა ინფორმაცია.
- **კონფიდენციალური ინფორმაცია -** პერსონალური და განსაკუთრებული კატეგორიის მონაცემი, ფინანსური, IT უსაფრთხოების მონაცემები ან სხვა ნებისმიერი ინფორმაცია, რომლის ხელყოფაც გამოიწვევს აპარატის ფუნქციონირების შეფერხებას, ზიანს, საფრთხეს, სახელმწიფო ინტერესების ან/და რეპუტაციის შელახვას. ასეთი ინფორმაცია შეიძლება იყოს დოკუმენტირებულად აღწერილი ან ელექტრონული ფორმით შენახული.
- **შიდასამსახურებრივი გამოყენების ინფორმაცია** - ეს არის ინფორმაცია, რომელიც გამოიყენება აპარატის საქმიანობის ეფექტურად წარმართვისთვის, შიდა კომუნიკაციის ფარგლებში, ასევე მიეკუთვნება მეთოდოლოგიურ დოკუმენტებს და როგორც წესი არ შეიცავს კონფიდენციალურ ინფორმაციას, თუმცა ამ ინფორმაციის ხელყოფა გამოიწვევს ორგანიზაციის ფუნქციონირების შეფერხებას და ზიანს.
- **საჯარო ინფორმაცია -** მონაცემები, რომლებიც არ მიეკუთვნება კონფიდენციალურ ან შიდასამსახურებდივ ინფორმაციას და არის ღია ნებისმიერი პირისათვის.
- **ინფორმაციული აქტივი** - აპარატში არსებული სხვადასხვა ინფორმაციის ერთობლიობა, რომლითაც შესაძლებელია ინფორმაციის გაგება, გაზიარება, დაცვა და გამოყენება. აქტივები მოიცავს ნებისმიერ ტექნიკას და ინფორმაციულ სისტემას, ასევე სხვა ტიპის ინფორმაციის მატარებელ აქტივს, მათ შორის ფიზიკურ დოკუმენტაციას, მობილურ ტელეფონებში დაცული სამსახურებრივი ინფორმაციას, პორტატულ კომპიუტერებს, გარე მეხსიერების ბარათებს, მონაცემთა ბაზებს და ა.შ.
- **ინფორმაციული სისტემა** - მოიცავს ყველა სერვერს, ქსელის ინფრასტრუქტურას, სისტემას და პროგრამულ აპლიკაციას, ნებისმიერ ინფორმაციას, მონაცემთა ბაზებს, სხვა **კომპიუტერულ ქვესისტემებსა და კომპონენტებს,** რომლითაც სარგებლობს აპარატი ან არის მის საკუთრებაში ან რომელიც არის აპარატის პასუხისმგებლობის ქვეშ. ინფორმაციული სისტემების მოხმარება ასევე გულისხმობს შიდა და გარე სერვისების მოხმარებას. ინფორმაციული სისტემა არ მოიცავს პირად სარგებლობაში არსებულ მობილურ ტელეფონებს და ტელეფონით სოციალური ქსელებით სარგებლობას, გარდა სამსახურებრივი ელ-ფოსტისა.

4. ავტორიზაცია ინფორმაციული სისტემის გამოყენებისთვის

თანამშრომელს უფლება აქვს ინფორმაციული აქტივი გამოიყენოს მხოლოდ აპარატის მანდატთან და სამსახურებრივი მოვალეობების შესრულებასთან დაკავშირებული ამოცანების შესასრულებლად.

თანამშრომელს წვდომა აქვს მხოლოდ იმ ინფორმაციულ აქტივებთან, რომელზეც გაცემულია ავტორიზაცია შესაბამისი უფლებამოსილების მქონე პირის მიერ და რაც მათი უფლებამოსილების განხორციელებას უკავშირდება.

5. აქტივებზე პასუხისმგებლობა

თანამშრომლებს მათი სამსახურებრივი ფუნქციების შესაბამისად აქვთ დაშვება ინფორმაციულ აქტივზე. თანამშრომელი პასუხისმგებელია მისთვის გადაცემული ტექნიკის მოვლასა და პატრონობაზე, ასევე ინფორმაციის კონფიდენციალურობაზე, მთლიანობასა და ხელმისაწვდომობაზე.

6. აკრძალული მოქმედებები

თანამშრომელს ეკრძალება:

- IT სისტემების ადმინისტრატორის ნებართვის გარეშე პროგრამული უზრუნველყოფის დაყენება მის სარგებლობაში არსებულ კომპიუტერზე (რომელიც არ არის გათვალისწინებული პროგრამული უზრუნველყოფის მატრიცით), აღნიშნული შესაძლებელია განხორციელდეს ცენტრალიზებულად IT ადმინისტრატორის მიერ. ფოტო და ვიდეო ფაილების არამიზნობრივი გადმოწერა, ელექტრონული ფოსტით მასიური წერილების გაგზავნა (გარდა საერთაშორისო და პრ მიმართულებით მომუშავე თანამშრომლებისა), თამაში და ა.შ.
- სამსახურებრივი ელექტრონული მეილების გამოყენება პირადი მიზნებისთვის, მათ შორის ონლაინ ვაჭრობის, აპლიკაციებზე წვდომის მოპოვების და საიტებზე დარეგისტრირების ან სხვა პირადი მიზნებისათვის;
- უცხო პირებისაგან გამოგზავნილი მეილების და მიმაგრებული ფაილების გახსნა სათანადო შემოწმების და სანდოობაში დარწმუნების გარეშე;
- უცხო და საეჭვო მეილების სხვა თანამშრომლებისათვის გაგზავნა;
- სპამ მეილის ლინკებზე გადასვლა;
- წინასწარ ანტი ვირუსის მეშვეობით შემოწმების გარეშე მეხსიერების ბარათების და სხვა მოწყობილობების, რომლებიც განკუთვნილია მონაცემთა შესანახად და წასაკითხად გახსნა და გამოყენება;
- სამუშაო ადგილის დატოვება კომპიუტერის, დესტკოპის დაბლოკვის გარეშე, ხანმოკლედ პერიოდითაც კი; აღნიშნული შესაძლებელია განხორციელდეს ცენტრალიზებულადაც
- სხვებისათვის მომხმარებლის სახელის და პაროლ(ებ)ის გაზიარება პირდაპირი ან არაპირდაპირი გზით, გარდა IT ადმინისტრატორისა.
- სხვა პიროვნების მომხმარებლის სახელისა და პაროლის გამოყენება, გამონაკლისია საერთო ონლაინ რესურსებით სარგებლობის შემთხვევები.
- სხვა ნებისმიერი მესამე პირის (მათ შორის ოჯახის წევრები) დაშვება სამსახურებრივ კომპიუტერთან როდესაც კონფიდენციურ ან სხვების პერსონალურ ინფორმაციის შემცველი ინფორმაცია შეიძლება გახდეს მისთვის ხელმისაწვდომი;
- ისეთ აქტივობის განხორციელება, რომელიც მიმართულია ინფორმაციული სისტემის უსაფრთხოების კონტროლის მექანიზმების და დადგენილი აკრძალვების გვერდის ავლისკენ;
- ინფორმაციული აქტივების ისეთი გამოყენება, რაც იწვევს ინფორმაციული სისტემის მუშაობის შეფერხებას ან საფრთხეს უქმნის ინფორმაციის უსაფრთხოებას.

7. აქტივების გატანა

როგორც წესი დაუშვებელია ინფორმაციის, პროგრამული უზრუნველყოფისა თუ მოწყობილობის აპარატის შენობების გარეთ გატანა, გარდა იმ შემთხვევებისა რაც დადგენილია აპარატის ორგანიზაციული პოლიტიკით.

8. აქტივების დაბრუნება შრომითი ურთიერთობის დასრულების შემდეგ

შრომითი ურთიერთობის დასრულების შემდეგ, სამსახურებრივი მოვალეობის შესასრულებლად გამოყენებული ნებისმიერი მოწყობილობა, პროგრამული

უზრუნველყოფა ან ინფორმაცია შენახული ელექტრონულად ან ფიზიკურად, უნდა დაუბრუნდეს აპარატს.

9. ანტივირუსული დაცვა

ანტივირუსული პროგრამის (უსაფრთხოების დაცვის პროგრამული უზრუნველყოფის პაკეტი) დაყენება და განახლებების გააქტიურება სავალდებულოა ყველა კომპიუტერულ მოწყობილობაზე. აღნიშნული შესაძლებელია განხორციელდეს ცენტრალიზებულად IT ადმინისტრატორის მიერ.

10. პაროლების მართვა / პასუხისმგებლობა

თანამშრომელი ვალდებულია იხელმძღვანელოს პაროლების შერჩევისა და მოხმარების შემდეგი წესებით:

- **სავალდებულოა**, შეირჩეს რთული პაროლი, რომელიც უნდა შედგებოდეს:
    - მინიმუმ რვა სიმბოლოსგან
    - მინიმუმ ერთი ციფრისგან
    - მინიუმ ერთი დიდი და ერთი პატარა ასოსგან
    - მინიმუმ ერთი სპეციალური სიმბოლოსგან
    - სასურველია პაროლი არ იყოს სიტყვა ლექსიკონიდან, დიალექტური ან ჟარგონული სიტყვა ნებისმიერი ენიდან, ან ასეთი სიტყვა დაწერილი უკუღმა
    - პაროლი არ უნდა შედგებოდეს პირადი ინფორმაციის შემცველი ინფორმაციისგან (მაგ.: დაბადების თარიღი, მისამართი, ოჯახის წევრის სახელი და სხვა)
- დაუშვებელია პაროლების დაწერა/ამოწერა, გარდა იმ შემთხვევისა, როდესაც შენახვის უსაფრთხო მეთოდი შეთანხმებულია IT სისტემების ადმინისტრატორთან.
- დაუშვებელია მომხმარებლის პერსონალური პაროლების გაზიარება ნებისმიერი სახით (მათ შორის ვერბალურად, წერილობით, ელექტრონულად თუ სხვა ფორმით), გარდა IT ადმინისტრატორისა.
- აუცილებელია პაროლების შეცვლა თუ არსებობს საფუძვლიანი ეჭვი, რომ პაროლის ან სისტემის უსაფრთხოება დარღვეულია. ასეთ შემთხვევაში აუცილებელია დაფიქსირდეს უსაფრთხოების ინციდენტი.
- დაუშვებელია, ბოლო პაროლის ხელახლა გამოყენება.
- არ შეიძლება **პაროლის ღიად დაუცველ საქაღალდესა და ფაილში მითითება**
- სხვადასხვა სისტემაში სამუშაოდ უნდა იქნას გამოყენებული **სხვადასხვა პაროლი**
- პაროლები უნდა შეიცვალოს ყოველ 6 თვეში ერთხელ, აღნიშნულის უზრუნველყოფა შესაძლებელია განხორციელდეს ცენტრალიზებულად IT ადმინისტრატორის მიერ.
- პაროლი **აუცილებელია** შეიცვალოს სისტემაში პირველად შესვლის შემდეგ.
- რეკომენდირებულია პირადი მიზნებისთვის გამოყენებული პაროლები არ იქნას გამოყენებული სამსახურებრივი დანიშნულებისათვის.

აპარატის IT ადმინისტრატორმა შესაძლოა ცენტრალიზებულად შეზღუდოს რიგ პროგრამებზე წვდომის მიზნებისათვის მარტივი პაროლის გამოყენების შესაძლებლობა.

11. მონაცემების ასლების შენახვა

თანამშრომელი ვალდებულია შექმნას დოკუმენტის სარეზერვო ასლი **OneDrive** - ის ექაუნთზე იმ შემთხვევაში თუ სახეზეა ორი წინაპირობა:

- აღნიშნული ინფორმაცია არის მნიშვნელოვანი ინსტიტუციური მეხსიერების ან დაკისრებული ვალდებულებების შესრულებისათვის
- იგივე დოკუმენტი არ ინახება/არ არის ხელმისაწვდომი აპარატის სარგებლობაში არსებულ რომელიმე პროგრამული უზრუნველყოფის ბაზებში.

12. სუფთა მაგიდისა და ეკრანის წესი

12.1.1. სუფთა მაგიდის პოლიტიკა

თუ ავტორიზებული მომხმარებელი არ არის თავის სამუშაო მაგიდასთან, ყველა ნაბეჭდი დოკუმენტი, ასევე ყველა ინფორმაცია, რომელიც კონფიდენციალურია უნდა იქნას აღებული სამუშაო მაგიდიდან ან სხვა ადგილებიდან (პრინტერები, ფაქსი და ა.შ.), რომ თავიდან იქნას არიდებული არაავტორიზებული წვდომა ინფორმაციასთან.

ასეთი სახის დოკუმენტაცია უნდა ინახებოდეს უსაფრთხოდ, შესაბამისი წესების დაცვით.

12.1.2. სუფთა ეკრანის პოლიტიკა

თუ ავტორიზებული მომხმარებელი არ იმყოფება თავის სამუშაო მაგიდასთან, ეკრანზე არ უნდა იყოს ხელმისაწვდომი კონფიდენციალურია ინფორმაცია და არ უნდა იყოს თავისუფალი წვდომა სისტემებზე, რომელზეც ამ მომხმარებელს აქვს ავტორიზაცია. სამუშაო სივრცის მცირე დროით დატოვების შემთხვევაშიც კი მომხმარებელმა უნდა იზრუნოს ამ წესის დაცვაზე, მათ შორის მოახდინოს - switch user.

12.1.3. საერთო სარგებლობის მოწყობილობის დაცვა

დოკუმენტაცია, რომელიც შეიცავს კონფიდენციალურია ინფორმაციას დაუყოვნებლივ უნდა იქნას აღებული საერთო სარგებლობის მოწყობილობებიდან: პრინტერი, ფაქსი და ა.შ.

13. ინტერნეტის მოხმარება

IT სისტემების ადმინისტრატორი უფლებამოსილია ინდივიდუალურ მომხმარებელს, მომხმარებელთა ჯგუფებს ან ყველა თანამშრომელს შეუზღუდოს წვდომა გარკვეულ ვებ-გვერდებზე უსაფრთხოებიდან გამომდინარე. მომხმარებელს შეუძლია მოითხოვოს წვდომის დაშვება IT სისტემების ადმინისტრატორთან მოთხოვნის დაფიქსირებით. დაუშვებელია, თანამშრომლის მხრიდან ასეთ ვებ-გვერდზე წვდომის მოპოვება შეზღუდვის გვერდის ავლით, დამოუკიდებლად.

თანამშრომელმა არავერიფიცირებული ვებ-გვერდიდან მიღებული ინფორმაცია უნდა მიიჩნიოს არასანდოდ. ასეთი ინფორმაციის გამოყენება დასაშვებია მხოლოდ მას შემდეგ, რაც შემოწმდება მისი უტყუარობა და სანდოობა.

თანამშრომელი პასუხისმგებელია ყველა შესაძლო შედეგზე, რომელიც წარმოიშვება ინტერნეტ სერვისების არაავტორიზებული ან არასათანადო მოხმარების შედეგად.

14. ელ-ფოსტა და სხვა საკომუნიკაციო საშუალებები

გარდა ელ-ფოსტისა, შეტყობინების გაცვლის საშუალებას წარმოადგენს: Viber, WhatsApp, Signal, Facebook Messenger, მოკლე ტექსტური შეტყობინება და სხვ.

აკრძალულია გამაღიზიანებელი, სექსუალური შევიწროვების შინაარსის მქონე, უხეში, ცილისმწამებლური, ნებისმიერი სხვა მიუღებელი ან უკანონო მასალების გაგზავნა. აკრძალულია 'სპამ' შეტყობინებების დაგზავნა.

'სპამ' შეტყობინების მიღების შემთხვევაში, თანამშრომელი ვალდებულია აცნობოს IT სისტემების ადმინისტრატორს ან გადაიტანოს სპამ საქაღალდეში.

15. კომპიუტერული ტექნიკით სარგებლობის წესები

თანამშრომელი ვალდებულია, დაიცვას, გაუფრთხილდეს და მიზნობრივად გამოიყენოს კომპიუტერულ ტექნიკა, მათ შორის უზრუნველყოს გამოყენებული ტექნიკის პერიოდული ფიზიკური დასუფთავება, ჰიგიენა შესაბამისი ქიმიური საწმენდი საშუალებებით. დაკარგვის ან ფიზიკური დაზიანების შემთხვევაში თანამშრომელი ვალდებულია დაუყოვნებლივ აცნობოს აღნიშნული ადმინისტრაციულ და ფინანსურ დეპარტამენტს და წარადგინოს დეტალური ახსნა-განმარტება პირველი მოადგილის სახელზე. დაზიანებული ტექნიკის გამოცვლის მოთხოვნას თან უნდა ერთვოდეს დეტალური ახსნა-განმარტება ტექნიკის დაზიანების პირობების და ვითარების შესახებ, წინააღმდეგ შემთხვევაში მიიჩნევა რომ ტექნიკა დაზიანებულია გაუფრთხილებლობით, რასაც შესაძლოა მოყვეს კანონმდებლობით გათვალისწინებული სამართლებრივი შედეგები.

აუცილებელია განსაკუთრებული წესების დაცვა, როდესაც ლეპტოპი განთავსებულია ავტომობილში ან სხვა სატრანსპორტო საშუალებაში, საჯარო სივრცეში, სასტუმროს ოთახში, შეხვედრის ადგილას, საკონფერენციო დარბაზში ან სხვა დაუცველ ტერიტორიაზე აპარატის შენობის გარეთ.

პირი, რომელსაც გააქვს ლეპტოპი აპარატის შენობების ფარგლებს გარეთ, ვალდებულია დაიცვას შემდეგი წესები:

- ლეპტოპი არ შეიძლება დატოვებულ იქნას უმეთვალყურეოდ, შესაძლებლობის შემთხვევაში ის უნდა ჩაიკეტოს ან გამოყენებულ იქნას სპეციალური საკეტები ნივთის უსაფრთხოებისთვის.
- ლეპტოპის საჯარო სივრცეებში გამოყენების დროს, თანამშრომელი ვალდებულია არ დაუშვას ინფორმაციაზე წვდომა არაავტორიზებული პირების მხრიდან.

- სისტემების და პარამეტრების განახლებები სრულდება ავტომატურად, სადაც ეს შესაძლებელია IT სისტემების ადმინისტრატორის მიერ ან თანამშრომლების მიერ ხელით.
- ანტივირუსული პროგრამის დაყენება და განახლება ხდება ავტომატურ რეჟიმში.

რეკომენდირებულია არ იქნას გამოყენებული საჯარო და ნაკლებად დაცული ინტერნეტი.

16. დისტანციური მუშაობა

დისტანციური მუშაობა გულისხმობს საინფორმაციო და საკომუნიკაციო მოწყობილობების საშუალებით თანამშრომლის მიერ სამუშაოების შესრულებას აპარატის ფარგლებს/შენობის გარეთ.

17. ინფორმაციისა და საკომუნიკაციო სისტემების მოხმარების მონიტორინგი

მონაცემები, რომლებიც იქმნება, ინახება, იგზავნება ან მიღებულია ინფორმაციული სისტემებისა და აპარატის სხვა საკომუნიკაციო სისტემების საშუალებით, როგორიცაა სხვადასხვა აპლიკაციები, ელ.ფოსტა, ინტერნეტი და ა.შ., მისი დანიშნულების მიუხედავად ითვლება აპარატის საკუთრებად.

ინფორმაციული უსაფრთხოების მაღალი ინტერესიდან გამომდინარე აპარატის შესაბამის უფლებამოსილ პირებს აქვთ წვდომა ასეთი სახის მონაცემებთან და აღნიშნული წვდომა არ ითვლება მომხმარებლების კონფიდენციალურობის დარღვევად.

აპარატს შეუძლია გამოიყენოს ხელსაწყოები კომუნიკაციის აკრძალული მეთოდების იდენტიფიცირების, დაბლოკვისა ან/და აკრძალული შინაარსის გაფილტვრის მიზნით.

18. ინფორმაციულ აქტივზე წვდომის კონტროლი

აპარატში ინფორმაციაზე წვდომა თანამშრომლებს გააჩნია მათი სამსახურებრივი მოვალეობების გათვალისწინებით.

როგორც წესი, აპარატის თანამშრომელი თავის საქმიანობას რამდენიმე პროგრამული უზრუნველყოფის მეშვეობით ახორციელებს, რომლებსაც ყავს გარე ადმინისტრატორი, მაგალითად Callapp; e-DOC; eHRMS; ფინანსთა სამინისტროს ელექტრონული სერვისების პორტალი და ა.შ.

სხვადასხვა პროგრამებით სარგებლობის და მომხმარებლებად დარეგისტრირების დროს თანამშრომლისთვის პრივილეგიების მინიჭება ხდება მათი პოზიციის და უფლებამოსილების ფარგლების გათვალისწინებით პროგრამის ადმინისტრატორის მიერ თითოეული ამ პროგრამის სარგებლობის წესების შესაბამისად.

შრომით სამართლებრივი ურთიერთობის შეწყვეტის ან სამსახურებრივ უფლებამოსილების ფარგლების ცვლილების დროს აპარატის შესაბამისი პასუხისმგებელი პირი (შესაბამისი სტრუქტურული ერთეულის ხელმძღვანელ სადაც მუშაობს/მუშაობდა თანამშრომელი)

ვალდებულია 1 სამუშაო დღის განმავლობაში იზრუნოს შესაბამის პროგრამებზე წვდომის გაუქმებასა ან შეცვლაზე.

19. ინფორმაციის კლასიფიკაცია

აპარატში თანამშრომლებს მათი უფლებამოსილების და კომპეტენციის შესაბამისად გააჩნიათ წვდომა კონფიდენციალურ, შიდასამსახურებრივ და საჯარო ინფორმაციაზე.

აღნიშნული ინფორმაცია შემდეგნაირად დაჯგუფდება:

კონფიდენციალურობის დონე	*მარკირება (შესაძლოა იქნეს გამოყენებული სხვადასხვა ფორმით)*	*კლასიფიკაციის კრიტერიუმი*	*წვდომის შეზღუდვა*
საჯარო	(მარკირების გარეშე)	ინფორმაციის გასაჯაროება ზიანს არ მიაყენებს აპარატს	ინფორმაცია ხელმისაწვდომია ყველასთვის
შიდა მოხმარების	შიდა მოხმარების	ინფორმაციაზე არაავტორიზებულმა წვდომამ შესაძლოა გამოიწვიოს აპარატისათვის ზიანის მიყენება აპარატში	ინფორმაცია ხელმისაწვდომია ყველა დასაქმებული პირისთვის და ავტორიზებული მესამე პირისათვის
კონფიდენციალური	კონფიდენციალური	ინფორმაციაზე არაავტორიზებულმა წვდომამ შესაძლოა გამოიწვიოს მნიშვნელოვანი ზიანი აპარატისათვის	ინფორმაცია ხელმისაწვდომია მხოლოდ კონკრეტულ პირებზე კანონმდებლობით დადგენილი წესით

20. ინციდენტები

თითოეული თანამშრომელი, რომელიც კავშირშია აპარატის მონაცემებთან და/ან სისტემებთან, ვალდებულია შეატყობინოს აპარატის უფლებამოსილ პირებს სისტემის ნებისმიერი სისუსტის, ინციდენტის ან მოვლენის შესახებ.

IT სისტემების ადმინისტრატორი რომელმაც მიიღო შეტყობინება უსაფრთხოების სისუსტის ან მოვლენის შესახებ, ახდენს მიღებული ინფორმაციის ანალიზს, ადგენს გამომწვევ მიზეზს და საჭიროების შემთხვევაში იღებს პრევენციულ ზომებს ხარვეზის გამოსწორების მიზნით.