სსიპ "საფინანსო-ანალიტიკური სამსახური"

ინფორმაციული უსაფრთხოების პოლიტიკა მესამე მხარეებისთვის

დოკუმენტის დასახელება:	ინფორმაციული უსაფრთხოების პოლიტიკა მესამე მხარეებისთვის
დოკუმენტის ტიპი:	პოლიტიკა
დოკუმენტის #:	IS-PL/05-25
ვერსია:	1
დოკუმენტზე პასუხისმგებელი პირი:	ინფორმაციული უსაფრთხოების მენეჯერი
დამტკიცებაზე უფლებამოსილი პირი:	სსიპ “საფინანსო-ანალიტიკური სამსახურის” უფროსი
კლასიფიკაციის დონე:	საჯარო

დოკუმენტის ცვლილებების ისტორია

ვერსია	დოკუმენტზე პასუხისმგებელი პირი	ცვლილების აღწერა	დამტკიცების თარიღი
1	ინფორმაციული უსაფრთხოების მენეჯერი	თავდაპირველი ვერსია	

სარჩევი

მუხლი 1. შესავალი

1. საქართველოს ფინანსთა სამინისტროს სსიპ "საფინანსო-ანალიტიკური სამსახური“ (შემდგომში „სამსახური“) 2010 წლის აპრილში შეიქმნა. სამსახურს ერთ-ერთი წამყვანი პოზიცია უკავია ქვეყნის საინფორმაციო-საკომუნიკაციო ტექნოლოგიების სფეროში. სამსახური მომსახურებას უწევს ფინანსთა სამინისტროს (შემდგომში „სამინისტრო“) ცენტრალურ აპარატსა და მის სისტემაში შემავალ დაწესებულებებს: სახაზინო სამსახურს, შემოსავლების სამსახურს, მომსახურების სააგენტოს, საგამოძიებო სამსახურს, ფინანსთა სამინისტროს აკადემიას, ასევე სხვა სახელმწიფო უწყებებსა და ორგანიზაციებს.
2. სამსახური ქმნის, ნერგავს და ავითარებს პროგრამული უზრუნველყოფის სისტემებს, როგორიცაა:

   ა) ბიუჯეტის მართვის სისტემა (eBudget);

   ბ) სახელმწიფო ხაზინის მომსახურების სისტემა (eTreasure);

   გ) სახელმწიფო ვალისა და საინვესტიციო პროექტების მართვის სისტემა (eDMS და DMFas);

   დ) ადამიანური რესურსების მართვის ელექტრონული სისტემა (eHRMS).

   ე) ვიზიტორთა მართვის ელექტრონული სისტემა (eVMS)

   ვ) საქმისწარმოების ავტომატიზებული სისტემა (eDoc)

   ზ) საჯარო სამსახურის ვაკანსიების მართვის სისტემა (hr.gov.ge)

   თ) ელექტრონული აუქციონის სისტემა (eAuction)

   ი) მომხმარებლებისა და დაშვებების მართვის სისტემა (ePassport)

   კ) საინვესტიციო პროექტების მართვის სისტემა (ePim)

   ლ) ავტოსატრანსპორტო საშუალებების აღრიცხვისა და მართვის სისტემა (eVMS)

   მ) გარემოსდაცვითი ინფორმაციის მართვის სისტემა (EIMS)

   ნ) ბუღალტრული აღრიცხვისა და ანგარიშგების, აუდიტის ზედამხედველობის სამსახურის ელექტრონული სისტემა (SARAS).

   ო) და სხვა.

3. სამსახურის საქმიანობის ერთ-ერთი მიმართულება არის სამინისტროს სისტემის, სხვა სახელმწიფო უწყებებისა და ორგანიზაციების ვებგვერდების შემუშავება და სამინისტროს შიდა კორპორაციული ელექტრონული სივრცის განვითარება.
4. სამსახური მომხმარებელს სთავაზობს სხვადასხვა სერვისს, მათ შორის, eCloud - ღრუბლოვან გამოთვლით ტექნოლოგიებს, რომელიც საშუალებას იძლევა ნებისმიერი ორგანიზაციის სერვერული ინფრასტრუქტურა განთავსდეს სამსახურის ინფრასტრუქტურაში და თვიდან იქნას აცილებული ის პრობლემები და ხარჯები, რაც დამკვეთის ლოკალური ინფრასტრუქტურის შეძენას, შენახვასა და მართვასთან არის დაკავშირებული.
5. ციფრული მომსახურებების განვითარებასთან ერთად, მონაცემთა უსაფრთხოება და კონფიდენციალურობის დაცვა სამსახურისთვის პრიორიტეტული გახდა. სწორედ ამ მიზეზით, სამსახურში მიმდინარეობს ინფორმაციული უსაფრთხოების მართვის საერთაშორისო სტანდარტის – ISO/IEC 27001:2022-ის დანერგვა. სტანდარტის დანერგვის მიზანია:
   ა) მომხმარებელთა ნდობის გაძლიერება

ბ) კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის (CIA) უზრუნველყოფა
გ) კიბერუსაფრთხოების რისკების შემცირება
დ) შესაბამისობა საერთაშორისო და ადგილობრივ რეგულაციებთან
ე) ბიზნეს პროცესების ოპტიმიზაცია და ინფორმაციული უსაფრთხოების მმართველობის გაუმჯობესება
ვ) მონაცემთა გაჟონვისა და ინფორმაციული ინციდენტების პრევენცია
ზ) მომწოდებლებთან და პარტნიორებთან უსაფრთხო ურთიერთობები

6. წინამდებარე დოკუმენტი (შემდგომში „პოლიტიკა“) აღწერს სამსახურის ინფორმაციული უსაფრთხოების მართვის პროცესებს, რომელთა მიზანია უზრუნველყოს მონაცემთა და IT რესურსების დაცვა უსაფრთხოების პრინციპების – კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის (CIA) – შესაბამისად.

პოლიტიკა წარმოადგენს სამსახურის მიერ მიღებული პოლიტიკების, პროცესებისა და საუკეთესო პრაქტიკების ჩამონათვალს, რომელიც უზრუნველყოფს ინფორმაციული აქტივების დაცვის მაღალი სტანდარტების დაცვას.

მუხლი 2: მიზანი

წინამდებარე პოლიტიკის მიზნებია:
ა) სამსახურის ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) სტრუქტურირებული აღწერა;
ბ) სამსახურის შიგნით ინფორმაციული უსაფრთხოების მართვის პროცესების განმარტება და რეგულირება;
გ) სამსახურის პარტნიორი ორგანიზაციების ინფორმირება ინფორმაციული უსაფრთხოების მოთხოვნებზე;

შენიშვნა: წინამდებარე დოკუმენტში აღწერილი არის სამსახურში არსებული ზოგადი პრაქტიკა და, სამსახურის ინტერესებიდან გამომდინარე, არ არის დასახელებული კონკრეტული ხელსაწყოები, რომელიც უზრუნველყოფს ინფორმაციული უსაფრთხოების რისკების შემცირებას.

მუხლი 3. ტერმინთა განმარტება

1. პოლიტიკაში გამოყენებული ინფორმაციული უსაფრთხოების ტერმინები და მათი განმარტებები:

ა) ISO/IEC 27001:2022 – საერთაშორისო სტანდარტი, რომელიც განსაზღვრავს ინფორმაციული უსაფრთხოების მართვის სისტემის მოთხოვნებს ორგანიზაციებში.

ბ) იუმს – ინფორმაციული უსაფრთხოების მართვის სისტემა, რომელიც მოიცავს პოლიტიკებს, პროცესებსა და კონტროლის მექანიზმებს ინფორმაციული უსაფრთხოების უზრუნველსაყოფად.

გ) კონფიდენციალურობა – მონაცემებზე წვდომა მხოლოდ უფლებამოსილი პირებისთვის.

დ) მთლიანობა – მონაცემების სიზუსტისა და სანდოობის შენარჩუნება.

ე) ხელმისაწვდომობა – ინფორმაციის დროული და უწყვეტი ხელმისაწვდომობა ავტორიზებული პირებისთვის.

ვ) რისკის მართვა – პროცესების ერთობლიობა, რომელიც გამოიყენება ინფორმაციული უსაფრთხოების რისკების იდენტიფიცირებისთვის, შეფასებისა და მოპყრობისათვის.

ზ) ნარჩენი რისკი – რისკი, რომელიც რჩება რისკების მოპყრობის შემდეგ.

თ) ფიზიკური უსაფრთხოება – უსაფრთხოების ზომები, რომლებიც იცავს ფიზიკურ აქტივებს, მონაცემთა ცენტრებსა და მოწყობილობებს.

ი) წვდომის კონტროლი – პროცესი, რომლებიც განსაზღვრავს, ვის, როდის და როგორ შეუძლია წვდომა IT სისტემებსა და მონაცემებზე.

კ) ავთენტიფიკაცია – პროცესი, რომელიც უზრუნველყოფს მომხმარებლის, ან სისტემის იდენტობის გადამოწმებას (მაგ., პაროლით, ბიომეტრიით, ორფაქტორიანი ავთენტიფიკაციით).

ლ) ავტორიზაცია – პროცესი, რომელიც განსაზღვრავს, აქვს თუ არა მომხმარებელს უფლება კონკრეტული ქმედებების განხორციელებაზე.

მ) მონაცემთა კლასიფიკაცია – ინფორმაციის კატეგორიზაცია მისი კრიტიკულობისა და დაცვის საჭიროების მიხედვით (მაგ., საჯარო, კონფიდენციალური, საიდუმლო).

ნ) შიფრაცია – მონაცემთა კოდირების მეთოდი კრიპტოგრაფიის გამოყენებით, რომელიც უზრუნველყოფს, რომ ინფორმაცია ხელმისაწვდომი იყოს მხოლოდ უფლებამოსილი პირებისთვის.

ო) ინფორმაციული უსაფრთხოების ინციდენტი (შემდგომში „ინციდენტი“) – ნებისმიერი მოვლენა, რომელიც საფრთხეს უქმნის ინფორმაციულ უსაფრთხოებას (მაგ., მონაცემთა გაჟონვა, DDoS შეტევა, სისტემაში არაუფლებამოსილი წვდომა).

პ) ინციდენტების მართვა – პროცესი, რომელიც უზრუნველყოფს ინციდენტების დროულ აღმოჩენას, ეფექტიან რეაგირებას, გამოძიებასა და აღმოფხვრას.

ჟ) SIEM (Security Information and Event Management) – უსაფრთხოების ინფორმაციისა და მოვლენების მართვის სისტემა, რომელიც აგროვებს და აანალიზებს სერვერული, ქსელური და უსაფრთხოების სისტემების ლოგებსა და ინციდენტებს.

რ) მესამე მხარის რისკი – რისკი, რომელიც დაკავშირებულია პარტნიორების, მომწოდებლების ან სხვა იურიდიული, თუ ფიზიკური პირების მიერ მოწოდებულ სერვისებთან ან/და პროდუქტებთან.

ს) ბიზნეს უწყვეტობა – პროცესების ერთობლიობა, რომელიც უზრუნველყოფს სამსახურის საქმიანობის უწყვეტ ოპერირებას კრიზისის დროს.

ტ) DLP (Data Leak Prevention) – მონაცემთა გაჟონვის პრევენციის სისტემები, რომლებიც ხელს უშლის არაუფლებამოსილ წვდომასა და მონაცემთა გაჟონვას.

უ) PAM (Privileged Access Management) - სისტემა, რომელიც უზრუნველყოფს კრიტიკულ სისტემებზე პრივილეგირებული წვდომებისა და მომხმარებლების მართვასა და მონიტორინგს.

ფ) მესამე მხარე - ორგანიზაცია ან პირი, რომელიც არ არის უშუალოდ დაკავშირებული სამსახურის შიდა საქმიანობებთან, მაგრამ არის ჩართული ან გავლენას ახდენს მის პროცესებზე, სერვისებზე ან ინფორმაციაზე. მესამე მხარე შეიძლება იყოს გარე მიმწოდებელი, პარტნიორი, ან სერვისის პროვაიდერი, რომელსაც სამსახური ენდობა გარკვეული სერვისების, პროდუქტების ან მხარდაჭერის მიწოდებაში.

მუხლი 4. ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს)

1. ინფორმაციული უსაფრთხოები მართვის მიზნით სამსახურში შეიქმნა ინფორმაციული უსაფრთხოების საბჭო, რომელიც დაკომპლექტებული არის სამსახურის უფროსისა და სხვადასხვა სტრუქტურული ერთეულების ხელმძღვანელებით. სამსახურში ინფორმაციული უსაფრთხოების ყოველდღიურ პროცესებზე პასუხისმგებელი არის ინფორმაციული უსაფრთხოების მენეჯერი.
2. სამსახურში დანერგილი არის ისეთი ძირითადი პროცესები, როგორიც არის:
   ა) ინფორმაციული აქტივების ინვენტარიზაცია
   ბ) ინფორმაციული უსაფრთხოების რისკების შეფასება და სამოქმედო გეგმის განსაზღვრა
   გ) ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების ყოველდღიური მონიტორინგი
   დ) ინფორმაციული უსაფრთხოების რისკების შეფასება ახალ პროექტებში
   ე) წვდომის გადახედვის პროცესი ძირითად ინფორმაციულ სისტემებში.
   ვ) თანამშრომლებისთვის ინფორმაციული უსაფრთხოების ცნობიერების ასამაღლებელი აქტივობები
3. სამსახურში დოკუმენტირებული და საჭიროების შემთხვევაში თანამშრომლებთან მიწოდებულია ყველა საჭირო პოლიტიკა და პროცედურა ინფორმაციული უსაფრთხოები მართვის ჭრილში
4. თანამშრომლებთან და მესამე მხარეებთან ურთიერთობაში გათვალისწინებულია კონფიდენციალურობის, პერსონალური მონაცემების დაცვის საკითხები.

მუხლი 5. ქსელის უსაფრთხოება

1. ქსელის უსაფრთხოების ეფექტური მართვა ISO 27001 სტანდარტის შესაბამისად მოიცავს სხვადასხვა კონტროლის მექანიზმებს, რომელთა მიზანია ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის (CIA) დაცვა. ამ მიზნით სამსახურში დანერგილია შემდეგი კონტროლის მექანიზმები:
   ა) სამსახურის შიდა ქსელი არის სეგმენტირებული - ერთმანეთისგან გამიჯნულია მომხმარებლების და სერვერული ქვე-ქსელები. ქვე-ქსელებს შორის კომუნიკაცია ხორციელდება Firewall-ის გავლით.
   ბ) სამსახურის გარე ქსელის პერიმეტრი დაცულია კომერციული და ვენდორის მიერ მხარდაჭერილი NG Firewall-თ, რომელსაც აქვს IPS/IDS, Antivirus, URL Filtering ფუნქციონალი და ისინი დაკონფიგურირებულია სამსახურის შიდა პოლიტიკების და იდენტიფიცირებული რისკების შესაბამისად.
   გ) სამსახურის თანამშრომლებს კორპორატიული ლეპტოპებიდან შიდა სერვერულ რესურსებზე დისტანციური წვდომა აქვთ კორპორატიული VPN სისტემის გამოყენებით.
   დ) ქსელური მოწყობილობების გენერირებული ლოგების თავმოყრა ხორციელდება SIEM სისტემაში, რომლის ყოველდღიურ მონიტორინგს ახორციელებს კომპიუტერული უსაფრთხოების სპეციალისტი
   ე) ქსელური კომუნიკაციის დროს გამოყენებულია TLS 1.2/1.3 შიფრაციის მექანიზმები.
   ვ) ხორციელდება ქსელური მოწყობილობების ოპერაციული სისტემების განახლებების პერიოდული ინსტალაცია ახალი, კრიტიკული სისუსტის, ან ხარვეზის აღმოსაფხვრელად.

მუხლი 6. იდენტობისა და წვდომის კონტროლის პროცესი

1. იდენტობისა და წვდომის კონტროლის პროცესის მიზანია უზრუნველყოს, რომ მხოლოდ უფლებამოსილ მომხმარებლებს, სისტემებსა და აპლიკაციებს ჰქონდეთ წვდომა სამსახურის იმ IT რესურსებზე და იმ მინიმალური წვდომის დონით, რომელიც საჭიროა მათი ფუნქციების შესასრულებლად. ეს პროცესი ხელს უწყობს ინფორმაციული აქტივების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის (CIA) დაცვას.
2. სამსახურში კრიტიკულ ბიზნეს აპლიკაციებად ითვლება ისეთი სისტემები, რომლებიც გამოყენებულია, ერთი მხრივ, პროგრამული უზრუნველყოფის განვითარების კუთხით და, მეორე მხრივ, ადმინისტრაციულ საქმიანობაში.
3. თითოეულ სისტემაში მომხმარებლებს აქვთ ინდივიდუალური მომხმარებლის სახელი და სამსახურის პაროლების პოლიტიკის შესაბამისი რთული პაროლი, რომელიც სავალდებულო წესით იცვლება პერიოდულად.
4. სამსახურში დანერგილია სრულყოფილი Onboarding/Offboarding პროცესი, რაც გულისხმობს თანამშრომლებისთვის საჭირო წვდომების მინიჭებას საჭიროებების მიხედვით, ასევე წასული თანამშრომლებისთვის წვდომის დროულ გაუქმებას არაავტორიზებული, წვდომის რისკის შესამცირებლად. მინიმუმ წელიწადში ერთხელ ინფორმაციული უსაფრთხოების მენეჯერის მხრიდან ხორციელდება წვდომის უფლებების გადახედვა.
5. ზემოაღნიშნულ თითოეულ სისტემას ჰყავს შესაბამისი პასუხისმგებელი პირი, რომლებიც უზრუნველყოფენ წვდომის მინიჭებისა და გაუქმების პროცესს მინიმალური წვდომის პრინციპის შესაბამისად.
6. სერვერულ ინფრასტრუქტურაზე წვდომისას სავალდებულო წესით გამოიყენება ორდონიანი ავთენტიფიკაციის მექანიზმი (2FA) არაავტორიზებული წვდომის რისკის მინიმიზირებისათვის.
7. თანამშრომელთა სამსახურში აყვანის წინ ხორციელდება ე.წ. Background Check, რომლის მიზანიცაა, შეფასდეს რამდენად კვალიფიციური და რელევანტურია თანამშრომელი სამსახურის მოთხოვნების და ბიზნეს პროცესების მიმართ. საჭიროების შემთხვევაში (დეველოპერები) წერენ შესაბამის ტესტს რათა გაიზომოს მათი ტექნიკური კომპეტენციის დონე.
8. პრივილეგირებული მომხმარებლების კონტროლისთვის სამსახურში დანერგილი არის პრივილეგირებული მომხმარებლების მართვის კონტროლის მექანიზმი (PAM).

მუხლი 7. ცვლილებების მართვის პროცესი

1. ცვლილებების მართვის პროცესი (Change Management) წარმოადგენს კრიტიკულ პროცესს ინფორმაციული ტექნოლოგიების, ბიზნეს ოპერაციების და უსაფრთხოების მართვისთვის. მისი მიზანია, უზრუნველყოს ცვლილებების უსაფრთხო, სტრუქტურირებული და კონტროლირებადი განხორციელება, რაც სამსახურს ეხმარება გარდაუვალი რისკების მინიმუმამდე დაყვანასა და სტაბილური ოპერაციების შენარჩუნებაში.
2. სამსახურში ორი სხვადასხვა ცვლილება განისაზღვრება, ეს არის:
   ა) ინფრასტრუქტურული ცვლილება IT სისტემებში
   ბ) Software Development-ის დროს განხორციელებული ცვლილება
3. სამსახურში პროგრამული პროდუქტების საწყისი კოდების სათავსოდ, ასევე ვერსიების კონტროლისთვის გამოიყენება ერთიანი სისტემა, სადაც წვდომა შეზღუდული არის უფლება-მოვალეობებისა და როლების შესაბამისად.
4. Software Development-ის პროცესში განსაზღვრული არის სხვადასხვა გარემო, კერძოდ:

ა) სატესტო გარემო – გარემო, სადაც ხდება აპლიკაციების ტესტირება რეალურ გარემოში გადატანამდე;
ბ) ე.წ. Pre-Production გარემო - გარემო სადაც ხდება ე.წ. Bug Fixing სანამ რეალურ გარემოში გადავა აპლიკაცია
გ) რეალური გარემო - გარემო სადაც განთავსებულია დახვეწილი და უშეცდომო აპლიკაცია, რომელიც შესაბამისობაშია დამკვეთის, ან მარეგულირებელ მოთხოვნებთან.

5. პროგრამული ცვლილებების ტესტირების ფაზაში ჩართულნი არიან ბიზნეს ანალიტიკოსები და აპლიკაციის ტესტერები, რომლებიც არიან პასუხისმგებელი კოდის უსაფრთხოებასა და აპლიკაციების სათანადო ფუნქციონირებაზე

მუხლი 8. სამუშაო გარემოს უსაფრთხოება

1. თანამშრომლების სამუშაო გარემოს უსაფრთხოებისათვის სამსახურში დანერგილი არის ისეთი კონტროლის მექანიზმები, როგორიცაა:
ა) ანტივირუსული დაცვა
ბ) პრივილეგირებული წვდომის შეზღუდვა
გ) წვდომის შეზღუდვა ინფორმაციის გარე მატარებლებზე
დ) კომპლექსური პაროლის გამოყენება
ე) ორ დონიანი ავთენტიფიკაციის მექანიზმი
ვ) განახლებების მართვის პროცესი
ზ) წვდომის შეზღუდვა არა საჭირო ვებ რესურსებზე
თ) VPN კავშირი დისტანციური წვდომისთვის (შეზღუდულად, მხოლოდ კრიტიკული აუცილებლობის შემთხვევაში)

მუხლი 9. მოწყვლადობებისა და განახლებების მართვა

სამსახურში დანერგილია:

1. მოწყვლადობების მართვის ავტომატიზებული სისტემა, რომლის მეშვეობითაც ხორციელდება კრიტიკული სისტემების რეგულარული სკანირება და რეპორტინგი.
2. განახლებების მართვის ავტომატიზებული სისტემა, რომლის მეშვეობითაც ხორციელდება განახლებების მაქსიმალურად ავტომატიზებული პროცესი: ჩამოტვირთვა-ტესტირება-ინსტალაცია სერვერებისა და სამომხმარებლო კომპიუტერებისათვის
3. იმ მოწყობილობებზე, სადაც განახლების ავტომატიზაცია შეუძლებელია, განახლებების მართვა ხორციელდება სამსახურის შესაბამის თანამშრომელთა მიერ.

მუხლი 10. ფიზიკური უსაფრთხოება

1. სამსახურის მისამართია, ქ. თბილისი, გორგასლის ქუჩა, #16
2. სამსახურს აქვს მონაცემთა დამუშავების ცენტრი, რომელშიც დანერგილია ფიზიკური და გარემოს უსაფრთხოების ყველა რელევანტური, სტანდარტით გათვალისწინებული კონტროლის მექანიზმი
3. სხვა, მოშორებულ ლოკაციაზე განთავსებულია მონაცემთა დამუშავების სარეზერვო ცენტრი, ასევე, ფიზიკური და გარემოს უსაფრთხოების შესაბამისი კონტროლის მექანიზმებით.

4. მონაცემთა დამუშავების ცენტრებს შორის უზრუნველყოფილია იზოლირებული და მაღალი სისწრაფის იზოლირებული ქსელური კავშირი დაცული ოპტიკურ-ბოჭკოვანი კაბელის საშუალებით.
5. მონაცემთა დამუშავების ცენტრები ფუნქციონირებს active-active რეჟიმში. დატაცენტრების კატასტროფის შემთხვევაში სისტემის აღდგენის დრო RTO (Recovery Time Objective) და აღდგენის წერტილი RPO (Recovery Point Objective) ნულის ტოლია. სისტემის მაღალმდგრადობას უზრუნველყოფს ჰიპერკონვერგენტული ტექნოლოგია.
6. სამუშაო გარემოში ფიზიკური დაშვებისას გამოიყენება ისეთი კონტროლის მექანიზმები, როგორიცაა:
   ა) პერიმეტრზე და სამსახურის ოფისის ოთახებში დაშვების სისტემა მაგნიტური ბარათის გამოყენებით
   ბ) ტურნიკეტი
   გ) დაცვის სამსახური
   დ) ვიდეო სამეთვალყურეო სისტემა, რომელზეც ხორციელდება უწყვეტი მონიტორინგი
7. მონაცემთა დამუშავების ცენტრებში დანერგილია შემდეგი კონტროლის მექანიზმები:
   ა) ხანძარქრობის სისტემა
   ბ) გაგრილების სისტემა
   გ) უწყვეტი კვების წყარო
   დ) გენერატორი
   ე) ფიზიკური დაშვების სისტემა მაგნიტური ბარათისა და ბიომეტრიული ავთენტიფიკაციის გამოყენებით, რომელზეც ხორციელდება უწყვეტი მონიტორინგი
   ვ) ვიდეო სამეთვალყურეო სისტემა, რომელზეც ხორციელდება უწყვეტი მონიტორინგი
   ზ) დაცვის სამსახური

მუხლი 11. აპლიკაციების უსაფრთხოება

1. აპლიკაციების უსაფრთხოება წარმოადგენს კრიტიკულ ელემენტს სამსახურის მიერ შემუშავებული პროგრამული უზრუნველყოფისთვის.
2. აპლიკაციების უსაფრთხოების ძირითადი პრინციპები, რომლებიც დაცულია Software Development-ის დროს:
   ა) OWASP Top 10-ის დაცვა – აპლიკაციები დაცულია ყველაზე გავრცელებული კიბერსაფრთხეებისგან (SQL Injection, XSS, CSRF და სხვა).
   ბ) შიფრაცია (Encryption) – მონაცემები დაცულია გადაცემისას (In-Transit).
   გ) Zero Trust Authentication – მხოლოდ ავთენტიფიცირებულ და ავტორიზებული მომხმარებლებს აქვთ წვდომა.
   დ) DevSecOps მიდგომა – უსაფრთხოების ავტომატიზირება ხდება CI/CD pipeline-ში.
3. ვებ აპლიკაციების უსაფრთხოების უზრუნველსაყოფად სამსახურში გამოიყენება Web Application Firewall

მუხლი 12. პერსონალური მონაცემების დაცვა

1. სამსახურზე ვრცელდება საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ“. შესაბამისად სამსახურში პერსონალური მონაცემების დაცვის კუთხით ზემოაღნიშნული კანონის მოთხოვნები არის დანერგილი.

2. სამსახურს ჰყავს პერსონალურ მონაცემთა დაცვის ოფიცერი, ასევე აქვს პერსონალური მონაცემების დაცვის პოლიტიკა, რომელიც ხელმისაწვდომია ყველა თანამშრომლისთვის
3. სამსახურის თანამშრომლებმა იციან:
   ა) თუ რა მონაცემები მუშავდება მათ შესახებ
   ბ) რა მიზნობრიობით მუშავდება პერსონალური მონაცემები
   გ) რა არის მათი, როგორც მონაცემთა სუბიექტების უფლებები
   დ) რამდენ ხანში ნადგურდება მათი პერსონალური მონაცემები
   ე) რომელ მესამე მხარეებს მიეწოდება მათი მონაცემები და რა მიზნით
   ვ) რა უსაფრთხოების ზომები არის მიღებული მათი პერსონალური მონაცემების დაცვის მიზნით
4. სამსახურში შემუშავებულია ვიდეო მეთვალყურეობის პოლიტიკა და შენობის პერიმეტრზე განთავსებულია შესაბამისი მანიშნებლები

მუხლი 13. პოლიტიკის დამტკიცება

1. პოლიტიკაში ცვლილებების შეტანა შესაძლებელია მხოლოდ ინფორმაციული უსაფრთხოების საბჭოს მიერ წარდგენილი რეკომენდაციის საფუძველზე სამსახურის უფროსის მიერ.
2. პოლიტიკა უნდა გადაიხედოს ყოველწლიურად
3. პოლიტიკა ძალაში შედის სამსახურის უფროსის მიერ მისი დამტკიცების დღიდან.