# ინფორმაციული უსაფრთხოების მართვის სისტემა

## 1. შესავალი

1. “თბილისის ელექტრომიმწოდებელი კომპანია "თელმიკო", თბილისის მოსახლეობისათვის, ელექტროენერგის მიწოდებას უზრუნველყოფს. კომპანია საქართველოს ენერგეტიკული ბაზრის რეფორმირების შედეგად შეიქმნა და 2021 წლის, 1 ივლისიდან თბილისში 719 ათას აბონენტს ემსახურება. ჩვენ დიდ ყურადღებას ვუთმობთ მომხმარებელთა უფლებების დაცვას.

2. „თელმიკო“ წარმოადგენს საქართველოს კრიტიკული ინფორმაციული სისტემების სუბიექტს, რა მიზნითაც დაინერგა ინფორმაციული უსაფრთხოების მართვის სისტემა.

3. ინფორმაციული უსაფრთხოების საჯარო პოლიტიკა წარმოადგენს „თელმიკოს“ მიერ მიღებული პოლიტიკების, დანერგილი პროცესებისა და საუკეთესო პრაქტიკების ჩამონათვალს, რომელიც უზრუნველყოფს ინფორმაციული აქტივების დაცვის მაღალი სტანდარტების დაცვასა და ჩვენი მომხმარებლების მონაცემების უსაფრთხოებას.

## 2. მიზანი

1. წინამდებარე პოლიტიკის მიზნებია:

   ა) „თელმიკოს“ ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) სტრუქტურირებული აღწერა;
   ბ) „თელმიკოში“ ინფორმაციული უსაფრთხოების მართვის პროცესების განმარტება და რეგულირება;
   გ) დაინტერესებული მხარეების ინფორმირება ინფორმაციული უსაფრთხოების მოთხოვნებზე;

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

## 3. ტერმინთა განმარტება

1. გამოყენებული ინფორმაციული უსაფრთხოების ტერმინები და მათი განმარტებები:

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 „თელმიკოს“ საქმიანობის უწყვეტ ოპერირებას კრიზისის დროს.
ფ) მესამე მხარე - ორგანიზაცია ან პირი, რომელიც არ არის უშუალოდ დაკავშირებული „თელმიკოს“ შიდა საქმიანობებთან, მაგრამ არის ჩართული ან გავლენას ახდენს მის პროცესებზე, სერვისებზე ან ინფორმაციაზე. მესამე მხარე შეიძლება იყოს გარე მიმწოდებელი, პარტნიორი, ან სერვისის პროვაიდერი, რომელსაც „თელმიკოს“ ენდობა გარკვეული სერვისების, პროდუქტების ან მხარდაჭერის მიწოდებაში.

## 4. ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს)

1. ინფორმაციული უსაფრთხოები მართვის მიზნით „თელმიკოში“ შეიქმნა ინფორმაციული უსაფრთხოების სამუშაო ჯგუფი (საბჭო), რომელიც დაკომპლექტებული არის სხვადასხვა სტრუქტურული ერთეულების ხელმძღვანელებით. ინფორმაციული უსაფრთხოების ყოველდღიურ პროცესებზე პასუხისმგებელი არის ინფორმაციული უსაფრთხოების მენეჯერი.

2. „თელმიკოში“ 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
ზ) წვდომის კონტროლი და სხვა

3. „თელმიკოში“ 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.

## 5. ქსელის უსაფრთხოება

1. კომპიუტერული ქსელის უსაფრთხოების ეფექტური მართვა ინფორმაციული უსაფრთხოების მართვის სისტემის შესაბამისად მოიცავს სხვადასხვა კონტროლის მექანიზმებს, რომელთა მიზანია ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის (CIA) დაცვა. ამ მიზნით დანერგილია შემდეგი კონტროლის მექანიზმები:

ა) „თელმიკოში“ შიდა ქსელი არის სეგმენტირებული - ერთმანეთისგან გამიჯნულია მომხმარებლების და სერვერული ქვე-ქსელები. ქვე-ქსელებს შორის კომუნიკაცია ხორციელდება Firewall-ის გავლით.
ბ) გარე ქსელის პერიმეტრი დაცულია კომერციული და ვენდორის მიერ მხარდაჭერილი NG Firewall-თ, რომელსაც აქვს IPS/IDS, Antivirus, URL Filtering ფუნქციონალი და ისინი დაკონფიგურირებულია „თელმიკოს“ შიდა პოლიტიკების და იდენტიფიცირებული რისკების შესაბამისად.
გ) „თელმიკოს“ 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.

## 6. იდენტობისა და წვდომის კონტროლის პროცესი

1. იდენტობისა და წვდომის კონტროლის პროცესის მიზანია უზრუნველყოს, რომ მხოლოდ უფლებამოსილ მომხმარებლებს, სისტემებსა და აპლიკაციებს ჰქონდეთ წვდომა „თელმიკოს“ 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. „თელმიკოში“ 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 „თელმიკოს“ პაროლების პოლიტიკის შესაბამისი რთული პაროლი, რომელიც სავალდებულო წესით იცვლება პერიოდულად.

4. „თელმიკოში“ 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. 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.

## 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 „თელმიკოს“ ეხმარება გარდაუვალი რისკების მინიმუმამდე დაყვანასა და სტაბილური ოპერაციების შენარჩუნებაში.

2. „თელმიკოში“ ორი სხვადასხვა ცვლილება განისაზღვრება, ეს არის:

   ა) ინფრასტრუქტურული ცვლილება IT სისტემებში

   ბ) Software Development-ის დროს განხორციელებული ცვლილება

3. პროგრამული პროდუქტების საწყისი კოდების სათავსოდ, ასევე ვერსიების კონტროლისთვის გამოიყენება ერთიანი სისტემა, სადაც წვდომა შეზღუდულია 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) 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

## 8. სამუშაო გარემოს უსაფრთხოება

1. თანამშრომლების სამუშაო გარემოს უსაფრთხოებისათვის „თელმიკოში“ 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)

## 9. მოწყვლადობებისა და განახლებების მართვა

1. „თელმიკოში“ დანერგილია:

ა) მოწყვლადობების მართვის ავტომატიზებული სისტემა, რომლის მეშვეობითაც ხორციელდება კრიტიკული სისტემების რეგულარული სკანირება და რეპორტინგი.

ბ) განახლებების მართვის ავტომატიზებული სისტემა, რომლის მეშვეობითაც ხორციელდება განახლებების მაქსიმალურად ავტომატიზებული პროცესი: ჩამოტვირთვა-ტესტირება-ინსტალაცია სერვერებისა და სამომხმარებლო კომპიუტერებისათვის

## 10. ფიზიკური უსაფრთხოება

1. “თელმიკოს“ სათავო ოფისის მისამართია, ქ. თბილისი, 0186 ოთარ ჩხეიძის №10. ასევე თბილისის 6 სხვადასხვა უბანში განთავსებული არის მომსახურების ცენტრები.

2. სამუშაო გარემოში ფიზიკური დაშვებისას გამოიყენება ისეთი კონტროლის მექანიზმები, როგორიცაა:

ა) პერიმეტრზე და ოფისის ოთახებში დაშვების სისტემა მაგნიტური ბარათის გამოყენებით

ბ) ტურნიკეტი

გ) დაცვის სამსახური

დ) ვიდეო სამეთვალყურეო სისტემა, რომელზეც ხორციელდება უწყვეტი მონიტორინგი

3. 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

## 11. აპლიკაციების უსაფრთხოება

1. აპლიკაციების უსაფრთხოება წარმოადგენს კრიტიკულ ელემენტს „თელმიკოს“ 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.

## 12. პერსონალური მონაცემების დაცვა

1. „თელმიკოზე“ ვრცელდება საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ“.

2. „თელმიკოს“ ჰყავს პერსონალურ მონაცემთა დაცვის ოფიცერი, ასევე აქვს პერსონალური მონაცემების დაცვის პოლიტიკა, რომელიც ხელმისაწვდომია ყველა თანამშრომლისთვის

3. თანამშრომლების ინფორმირებულები არიან:

   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. შემუშავებულია ვიდეო მეთვალყურეობის პოლიტიკა და შენობის პერიმეტრზე განთავსებულია შესაბამისი მანიშნებლები