REPUBLIKA E SHQIPËRISË
ENTI RREGULLATOR I ENERGJISË

RREGULLORJA PËR SIGURINË KIBERNETIKE TË INFRASTRUKTURAVE KRITIKE NË SEKTORIN E ENERGJISË ELEKTRIKE

Miratuar me Vendimin e Bordit të ERE-s nr. 126, datë 30.07.2020

Neni 1
Autoriteti

Enti Rregullator i Energjisë ka ndër objektivat e përcaktuara në nenin 18 të ligjit nr. 43/2015 "Për Sektorin e Energjisë Elektrike" i ndryshuar, promovimin dhe krijimin e një tregu të brendshëm konkurrues të sigurt dhe miqësor ndaj mjedisit për të gjithë klientët dhe furnizuesit, duke siguruar kushtet e duhura për funksionimin e sigurt dhe të qëndrueshëm të rrjeteve të energjisë elektrike, në bashkëpunim të ngushtë me Komunitetin e Energjisë dhe autoritetet rregullatore të vendeve të tjera. ~~Neni 26 i ligjit nr. 43/2015, gjithashtu përcakton se, sistemi i energjisë elektrike operon si një sistem i integruar me procese të vazhdueshme prodhimi, transmetimi, shpërndarjeje dhe konsumi të energjisë elektrike.~~

ERE është gjithashtu autoriteti përgjegjës për rregullimin në sektorin e gazit natyror, bazuar në ligjin nr. 102/2015. Në përputhje me këtë ligj, objektivat e ERE-s në ushtrimin e funksioneve rregullatore janë: a) Promovimi i krijimit të një tregu të brendshëm konkurrues, të sigurt dhe miqësor ndaj mjedisit për të gjithë klientët dhe furnizuesit. Sigurimi i kushteve të duhura për funksionimin e sigurt dhe të qëndrueshëm të rrjeteve të gazit natyror, në bashkëpunim të ngushtë me Komunitetin e Energjisë dhe autoritetet rregullatore të vendeve të tjera.

Bazuar në sa më sipër ERE konsideron sigurinë kibernetike në sektorin e energjisë elektrike si element themelor për ruajtjen e sigurisë dhe integritetit të sistemit elektroenergjitik Shqiptar.

Neni 2
Qëllimi

Qëllimi i kësaj rregulloreje është të përcaktojë rregullat dhe masat që duhet të ndërmerren nga subjektet e Licen~~s~~cuara nga ERE në sektorin e energjisë elektrike dhe gazit natyror, të cilët kanë përgjegjësi të garantojnë sigurinë kibernetike në infrastrukturat kritike që zotërojnë dhe operojnë. Garantimi i sigurisë kibernetike në sistemin elektroenergjitik dhe gazit natyror siguron furnizimin e pandërprerë me energji elektrike dhe gaz natyror të konsumatorëve në vendin tonë.

Neni 3
Objekti

Kjo rregullore përcakton detyrimin e operatorëve që zotërojnë ose operojnë infrastrukturat kritike në sektorin e energjisë elektrike dhe gazit natyror për të vendosur dhe zbatuar masat e duhura gjatë projektimit, instalimit dhe funksionimit të rrjetit ose pajisjeve të përdorura prej tyre, në

mënyrë që të garantojnë sigurinë, disponueshmërinë, integritetin dhe funksionimin e qëndrueshëm të sistemit elektroenergjitik dhe gazit natyror. Operatorët duhet të paraqesin pranë ERE, sipas Shtojcës nr. 2 dhe Shtojcës nr. 3, raporte për çdo ndërhyrje të paplanifikuar, cënim ose incident në fushën e sigurisë, disponueshmërisë dhe integritetit të rrjeteve të tyre të komunikimit elektronik, si dhe çdo ndërhyrje, dëmtim që ka ndikim në funksionimin e rrjeteve dhe/ose të statusit të tyre të shërbimit.

Neni 4
Përcaktimi i Termave

Termat e përdorur në këtë rregullore do të kenë kuptimin e mëposhtëm. Çdo term tjetër i përdorur në rregullore do të ketë kuptimin e përcaktuar në ligjin nr. 43/2015 "Për Sektorin e Energjisë Elektrike" i ndryshuar, ose në ligjin nr.25 /~~2017~~ 2024 "Për Sigurinë Kibernetike".

1. **"CSIRT"** - është Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kompjuterike.
2. **"CSIRT" sektorial"** - është ekipi/ personi përgjegjës ndaj Incidenteve të Sigurisë Kibernetike, në strukturën e një operatori që administron infrastruktura kritike dhe të rëndësishme të informacionit.
3. **"Hapësirë kibernetike"** – është mjedisi digjital i aftë të krijojë, të procesojë dhe tëshkëmbejë informacionin e krijuar nga sistemet, shërbimet e shoqërisë së informacionit, si dhe rrjetet e komunikimit elektronik.
4. **"Incident i sigurisë kibernetike"** - është një ngjarje e sigurisë kibernetike, gjatë së cilës shkaktohet cënimi i sigurisë së shërbimeve ose sistemeve të informacionit e të rrjeteve të komunikimit dhe sjell një efekt real negativ.
5. **"Infrastrukturë kritike e informacionit"** - është tërësia e rrjeteve dhe sistemeve të informacionit, cënimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë dhe/ose mirëqenien ekonomike të qytetarëve dhe/ose funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.
6. **"Operator i infrastrukturës kritike të informacionit"** - është një person juridik, publik ose privat, që administron infrastrukturën kritike të informacionit dhe operon në sektorin e Energjisë Elektrike OST sh.a.,OSHEE sh.a., ~~dhe~~ KESH sh.a~~.~~., Kurum International sh.a. – Sistemi SCADA, Dragobia Energy– Sistemi SCADA, Prell Energy sh.p.k. – Sistemi SCADA, Power Elektrik Slabinje – Sistemi SCADA, Seka Hydropower – Sistemi SCADA, Devoll Hydropower sh.a. – Servera, switche, firewall, dhe Trans Adriatic Pipeline (TAP) – Sistemi SCADA.

6.1 "Infrastrukturat e rëndësishme të informacionit janë persona juridikë, publikë ose privatë, që administrojnë infrastrukturën e rëndësishme të informacionit dhe operojnë në sektorin e energjisë elektrike. Këto përfshijnë: Operatorin e Shpërndarjes së Energjisë Elektrike (OSHEE) me Data Center Primary, Data Center Disaster Recovery, Data Center Business Continuity, rrjetin midis Data Center PR, DR dhe BC, si dhe rrjetin midis qendrës së të dhënave dhe pikave të komandimit; Termocentralin Vlorë sh.a me Sistemin DCS; dhe HEC Vlushe me Sistemin SCADA."

7. **"Rrezik i sigurisë kibernetike"** - është një rrethanë ose një ngjarje, e identifikueshme në mënyrë të arsyeshme, e cila mund të shkaktojë cënimin e sigurisë së shërbimeve ose sistemeve të informacionit dhe të rrjeteve të komunikimit.
8. **"Siguria e informacionit"** - është sigurimi i konfidencialitetit, integritetit dhe

disponueshmërisë së informacionit.

9. **“Siguria kibernetike”** - është tërësia e mjeteve ligjore, organizative, teknike dhe edukative, me qëllim mbrojtjen e hapësirës kibernetike.
10. **“SKI”** – janë Sistemet e Komunikimit dhe Informacionit.
11. **“AKSK”** – është Autoriteti Kombëtar për ~~Certifikimin Elektronik dhe~~ Sigurinë Kibernetike.

Neni 5
Rregulla të përgjithshme dhe parime bazë

1. Rregullorja për sigurinë kibernetike në infrastrukturat kritike dhe ato të rëndësishme në sektorin e energjisë elektrike dhe të gazit natyror është hartuar bazuar në nenin 18 të Ligjit nr. 43/2015 “Për Sektorin e Energjisë Elektrike”, të ndryshuar, në nenin 15 të Ligjit nr. 102/2015 “Për Sektorin e Gazit Natyror”, në Ligjin nr. 25/2024 “Për Sigurinë Kibernetike” dhe Vendimin e Këshillit të Ministrave nr. 553, datë 15.07.2020, "Për miratimin e Listës së Infrastrukturave Kritike të Informacionit dhe të Listës së Infrastrukturave të Rëndësishme të Informacionit", të ndryshuar.

~~1. Rregullorja për sigurinë kibernetike në infrastrukturat kritike në sektorin e energjisë elektrike është hartuar bazuar në nenin 18 të Ligjit Nr. 43/2015 “Për Sektorin e Energjisë Elektrike” i ndryshuar, Ligjit nr.2/2017 “Për Sigurinë Kibernetike” dhe VKM Nr.553, datë 15.07.2020, "Për miratimin e Listës së Infrastrukturave Kritike të Informacionit dhe të Listës së Infrastrukturave të Rëndësishme të Informacionit", duke marrë parasysh që:~~

   ~~b.~~a. Qëllimi i ligjit Nr. 43/2015 “Për sektorin e energjisë elektrike” i ndryshuar është që përmes kuadrit teknik dhe ligjor të sigurohet furnizim i sigurt dhe i qëndrueshëm me energji elektrike ~~I~~ i konsumatorëve, në përputhje me zhvillimet teknologjike. Ligji nr.25/~~2017~~ 2024 “Për Sigurinë Kibernetike” ka për qëllim arritjen e një niveli të lartë mbrojtjeje të sigurisë kibernetike dhe gatishmërinë ndaj sulmeve kibernetike duke përcaktuar masat e sigurisë, të drejtat, detyrimet si dhe bashkëpunimin e ndërsjellë ndërmjet operatorëve të infrastrukturave kritike përfshirë në sektorin energjitik, përmes të cilave sigurohen shërbimet e ~~licensuara~~licencuara.

   ~~c.~~b. Operatori i infrastrukturave kritike në sektorin e energjisë elektrike dhe gazit natyror duhet të ndërmarrë masat e duhura proporcionale, me kosto efektive, teknike dhe organizative për garantimin e sigurisë rrjetit për të menaxhuar, adresuar, dhe trajtuar në mënyrën e duhur rreziqet që paraqiten për sigurinë e rrjeteve dhe të informacionit që ata menaxhojnë në përmbushje të aktiviteteve të tyre dhe duke respektuar rolet e tyre.

2. Ndër të tjera kjo rregullore shërben DR~~s~~AFT ~~i~~ dokument mbështetës për Operatorët e infrastrukturave kritike në përputhje me kërkesat e Ligjit nr. 25/~~2017~~ 2024 “Për Sigurinë Kibernetike”. Për infrastrukturat kritike dhe akteve nënligjore në zbatim të tij, si dhe vendos procese për të ndihmuar OIKI të demonstrojnë dhe të vërtetojnë se ata po menaxhojnë rreziqet e sigurisë kibernetike në lidhje me shërbimet e ofruara. Këto procese përfshijnë kryesisht:

a. **Vetëvlerësimi nga OIKI.**

   OIKI do të paraqesë vetëvlerësimin e tij në ERE bazuar në “Rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë (Miratuar me urdhër nr.22, datë

26.04.2018 të ~~AKCESK~~AKSK). Ky vetëvlerësim do të përmbajë një informacioni të detajuar dhe të plotë (duke përfshirë metodologjinë që ka përdorur për të realizuar vetëvlerësimin, mënyrën se si e ka aplikuar këtë metodologji rezultatet e vetëvlerësimit të cilat duhet të përfshijnë identifikimin e riskut si dhe procesin e zvogëlimit të riskut) të çdo rreziku domethënës të identifikuara dhe çdo propozim fillestar për trajtimin e rrezikut përfshirë deklarim për rezultatin e nxjerrë duke identifikuar atë si “Jo e arritur "ose" Pjesërisht e arritur " dhe “E Arritur”.

Ky informacion duhet të dorëzohet duke përdorur modelin e raportimit të vetëvlerësimit i cili gjendet në Shtojcën. Nr.1.

Pasi të paraqitet informacioni në ERE, nëse ERE e gjykon të arsyeshme, mund të hyjë në vlerësime dhe të kërkoj informacione të mëtejshme për çështjet e raportuar për të

realizuar vlerësimet përkatëse. Kjo mund të përfshijë një kërkesë për sqarime të mëtejshme mbi rezultatet e vetëvlerësimit që konsiderohen si "Jo e arritur" ose "Pjesërisht e arritur". Nëse informacioni që është dërguar në ERE është i paqartë ERE mund të kërkojë sqarime nga OIKI.

OIKI në çdo kohë mund të kërkojë që të konsultohet me ERE sa më shpejt të jetë e mundur nëse nuk është i sigurt për çështjet objekt raportimi. Pasi OIKI të ketë përfunduar vetëvlerësimin e tyre, OIKI duhet të marrin në konsideratë fushat për përmirësim.

Në vetëvlerësimin fillestar që do të realizohet nga OIKI, qëllimi kryesor është kryerja e një vetëvlerësim objektiv dhe bazuar në rezultatet e vetëvlerësimit OIKI duhet të zhvillojnë një plan përmirësimi, atje ku ato janë të nevojshme ose sipas prioriteteve të përcaktuara nga ERE. Çdo vlerësim sipas statusit respektiv i arritur ose jo do të shoqërohet me shpjegimet përkatëse për çdo konkluzion. ERE mund të kërkojë që raportet e vetëvlerësimeve të përgatitura nga OIKI të jenë të audituara.

b. **Identifikimi dhe hartimi i planit të masave duke pasur parasysh rreziqet e mundëshme dhe të identifikuara.**

Pas procesit për paraqitjen e Vetëvlerësimit të përcaktuar më lart, OIKI duhet të propozojnë planet e tyre të masave tek autoritetet kompetente. OIKI mund të kërkojë bashkëpunim me ERE siç përcaktohet më lart.

Planet e masave bazohen në vetëvlerësimet e OIKI duke identifikuar rreziqet në përputhje me procesin e tyre të menaxhimit të riskut dhe metodologjinë e riskut. Plani i përmirësimit duhet të përcaktojë planet e veprimit të sigurisë kibernetike që OIKI synon të marrë atje ku rreziku është vlerësuar më i lartë duke konsideruar nivelet e tolerancës ndaj rrezikut. Planet e masave mund të përfshijnë ndër të tjera masat afatshkurtra ose masa strategjike afatgjata, për të cilat duhet të rivlerësohet buxheti i OIKI përmes planifikimit të duhur të biznesit. ERE, rast pas rasti, mund të kërkojë rishikimin e planit të masave nga OIKI në mënyrë që t'i ndihmojë ata në prioritarizimin dhe planifikimin e mbrojtjes nga rreziku kibernetik.

c. **Identifikimi dhe rishikimi i planeve të investimeve, të cilat duhet të marrin në konsideratë nevojën për të zvogëluar rreziqet e identifikuara në pikën (2.b).**

OIKI duhet të zhvillojë një Sistem të Menaxhimit të Sigurisë së Informacionit, për të menaxhuar në mënyrën e duhur rreziqet kibernetike, në çdo hallkë të sistemit të furnizimit. Ky sistem do të sigurohet brenda afatit të përcaktuar nga ERE sipas analizës dhe propozimit të OIKI, dhe mund të përfshijë ndër të tjera angazhimin e ekspertëve në fushën e sigurisë së teknologjisë së informacionit si dhe trajnime të ndryshme. Afatet kohore për iniciativat dhe kundërmasat e sigurisë kibernetike do të jenë pjesë e plani të përmirësimit. Prioriteti i masave të sigurisë së rrjeteve për rreziqet e larta duhet të bazohet në raportin e vetëvlerësimit rast pas rasti.

3. Pas paraqitjes së planit të parë të vetëvlerësimit dhe përmirësimit, ERE mund të kryejë monitorime në OIKI dhe në vijim të rezultateve të monitorimit do të paraqesë me rekomandimet përkatëse.

Neni 6

Detyrimet e Operatorëve të Infrastrukturave Kritike dhe të Infrastrukturave të Rëndësishme të Informacionit ~~Detyrime të Operatorëve të Infrastrukturave Kritike~~

~~2.~~1. Për qëllime të kësaj rregulloreje detyrat e operatorëve të infrastrukturave kritike dhe të Infrastrukturave të Rëndësishme të Informacionit në sektorin energjitik dhe gazit natyror përfshijnë:

a. OIKI duhet të marrë masat teknike dhe organizative për të menaxhuar rreziqet që mund ti shfaqen e që lidhen me sigurinë e rrjetit dhe të sistemeve të informacionit në të cilat mbështetet shërbimi i ~~licensuar~~ licencuar nga ERE, me qëllim sigurimin e vazhdimësisë së shërbimeve objekt ~~licensimi~~licencimi, referuar "Rregullores mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë" (Miratuar me urdhër nr.22, datë 26.04.2018 të ~~AKCESK~~AKSK).

b. OIKI duhet të marrë masa për të parandaluar dhe minimizuar ndikimin e incidenteve që ndikojnë në sigurinë e rrjetit dhe sistemeve të informacionit të përdorura për sigurimin e shërbimit për të cilin janë licensuar nga ERE, me qëllim të sigurimit të vazhdimësisë së këtyre shërbimeve. Kategoritë e Incidenteve Kibernetike përcaktohen sipas "Rregullores për Kategoritë e Incidenteve Kibernetike si dhe formatin e elementët e raportimit (Miratuar me urdhërin nr. 62, datë 10.09.2018 të ~~AKCESK~~AKSK).

c. OIKI do të jenë përgjegjës për zbatimin e masave që garantojnë sigurinë kibernetike nga palët e treta që ofrojnë shërbime ose produkte të infrastrukturës kritike. Operatorët e rrjetit OST sh.a. dhe OSSH sh.a. do të jenë gjithashtu përgjegjës për zbatimin e masave të sigurisë kibernetike nga Përdoruesit respektiv të rrjetit.

d. OIKI ka për detyrë për të njoftuar incidentet pranë ERE dhe Autoritetit të përcaktuar në përputhje me Ligjin nr. 25 /~~2017~~ 2024 "Për Sigurinë Kibernetike". Njoftimi do të kryhet për çdo incident i cili ka një ndikim të rëndësishëm në vazhdimësinë e shërbimit dhe veprimarisë së licensuar.

~~3.~~2. Në përputhje me përcaktimet e pikës 1 të këtij neni, OIKI, do të raportojë periodikisht një herë në gjashtë muaj, brenda muajit Janar dhe Korrik për 6 - mujorin paraardhës, sipas Shtojcës 1 të kësaj rregulloreje për çështjet që lidhen me zbatimin e gërmës a, b dhe c të pikës 1 të këtij neni dhe në çdo rast tjetër do të njoftojë menjëherë dhe jo më vonë se 4 orë nga momenti i zbulimit të incidentit të sigurisë të identifikuar sipas gërmës d të pikës 1 të këtij neni.

~~4.~~3. Faktorët kryesorë për vlerësimin e realizimit nga Operatori të detyrave sipas kësaj rregulloreje do të monitorohen nga ERE. Në çdo rast ERE do të vlerësojë:

- nëse janë zbatuar apo jo masa të përshtatshme dhe proporcionale të sigurisë kibernetike sipas detyrave që ka OIKI.
- nëse incidentet i janë njoftuar ERE
- Frekuenca e ndodhjes së një incidenti sipas gërmës d, pika 1, të nenit 6 në vetvete nuk do të thotë se detyrimisht ka pasur një dështim nga një operator për të përmbushur detyrat

e tij të sigurisë.

- Brenda 30 ditëve nga ndodhja e një incidenti në infrastrukturat kritike, OIKI duhet të paraqesë një raport të përgjithshëm për ERE. Brenda 90 ditëve nga ndodhja e incidentit në infrastrukturat kritike, OIKI duhet të paraqesë në ERE një raport të detajur të hetimit të incidentit.
- ERE gjithashtu mund të kërkojë OIKI të dorëzojnë pranë ERE raporte të audituar në lidhje me hetimin e një incidenti të sigurisë kibernetike.

Neni 6/1
Detyrime të tjera

Operatorët e Infrastrukturave Kritike dhe të Infrastrukturave të Rëndësishme të Informacionit në sektorin e energjisë elektrike dhe gazit natyror veç detyrave të përcaktuara në nenin 6 të kësaj rregullore, do të marrin masa dhe për zbatimin e përcaktimeve të parashtruara më poshtë në këtë nen:

1. Zbatimin e masave të plota organizative dhe teknike të sigurisë kibernetike në sistemet e komunikimit dhe të informacionit (SKI) nëpërmjet:
   a. Mbrojtjes së infrastrukturave kritike të informacionit për garantimin e shërbimeve;
   b. Menaxhimit të aseteve të teknologjisë së komunikimit dhe informacionit;
   c. Kontrollit të vijueshëm të masave të sigurisë;
   d. Vlerësimit të vijueshëm të masave të sigurisë;
   e. Reflektimit të kërkesave të sigurisë në projektet e reja të sistemeve të komunikimit dhe informacionit;
   f. Zbatimit të teknologjive mbrojtëse;
2. Rritjen e përgjegjësisë së operatorëve të infrastrukturave kritike për sigurinë kibernetike nëpërmjet:
   a. Hartimit dhe zbatimit të rregullave dhe procedurave të sakta për strukturat përgjegjëse për sigurinë kibernetike në OIKI;
   b. Hartimit dhe zbatimin e formateve dhe mënyrave të raportimit të sulmeve kibernetike për strukturat përgjegjëse për sigurinë kibernetike në OIKI;
   c. Zhvillimit të kapaciteteve dhe strukturave të dedikuara për sigurinë kibernetike;
   d. Koordinimit ndërmjet strukturave për reagimin ndaj sulmeve kibernetike;
   e. Shkëmbimit të informacionit për sigurinë kibernetike;
3. Zhvillimin e nivelit dhe aftësive të specialistëve të sigurisë kibernetike dhe të përdoruesve të SKI-ve nëpërmjet:
   a. Rekrutimit dhe caktimit në detyrë të specialistëve për sigurinë e kibernetike;
   b. Trajnimit të vijueshëm të specialistëve, promovimi dhe certifikimi i tyre;

c. Konceptimit të trajnimit si një fushë komplekse ku të përfshihet reagimi ndaj incidenteve, testimet penetruese në sisteme, menaxhimi rrezikut, analizat e kërcënimit, mënyrat paralajmëruese;

d. Trajtimit të mbrojtjes kibernetike në programet e trajnimit të stafit përgjegjës të Operatorëve të Infrastrukturave kritike.

4. Rritjes së bashkëpunimit ndërmjet operatorëve të infrastrukturave kritike në fushën e energjisë elektrike përsa i përket sigurisë kibernetike nëpërmjet:

a. Bashkëpunimit në bazë të përcaktimeve të Politikës së Sigurisë së Mbrojtjes Kibernetike të Republikës së Shqipërisë;

b. Detyrimeve të ligjit nr. 25/~~2017~~ 2024 "Për sigurinë kibernetike";

c. Pjesëmarrje në trajnime për mbrojtjen kibernetike.

d. Shkëmbimit të informacionit të ndërsjelltë që lidhet me sigurinë kibernetike ndërmjet OIKI.

Neni 7
CSIRT Sektorial

Operatorët e infrastrukturës kritike të informacionit në sektorin e energjisë elektrike dhe gazit natyror do të përcaktojnë personat përgjegjës për koordinimin, ndjekjen dhe zbatimin e masave për sigurinë kibernetike. Këta përfaqësues do të jenë pjesë e Ekipit të Përgjigjes ndaj Incidenteve të Sigurisë Kompjuterike (CSIRT Sektorial). Përcaktimi i personave përgjegjës për sigurinë kibernetike duhet të bëhet brenda 3 muajve pas hyrjes në fuqi të kësaj rregulloreje. Gjithashtu Operatorët e infrastrukturës kritike të informacionit në sektorin e energjisë elektrike dhe gazit natyror do të hartojnë rregullat dhe mënyrën e funksionimit të CSIRT sektorial duke ju referuar edhe "Udhëzimit për Metodologjinë e Organizimit dhe Funksionimit të CSIRT-eve në Nivel Kombëtar (~~Neni 7. pika 3 e~~ Ligji~~t~~ Nr. 25/~~2017~~ 2024 "Për Sigurinë Kibernetike").

Neni 8
Raportimi

Operatorët e infrastrukturës kritike të informacionit në sektorin e energjisë elektrike dhe gazit natyror do të raportojnë menjëherë dhe jo më vonë se 4 orë nga momenti i zbulimit të incidentit të sigurisë për çdo rast që përbën një shkelje/ndërhyrje e cila ka cënuar sigurinë kibernetike të infrastrukturave kritike që i licencuari zotëron ose operon, si dhe të çdo shërbimi tjetër që operatori ka në përdorim nga palë të treta.

ERE, me paraqitjen e informacioneve nga të licencuarit në rast të incidenteve të raportuara, do të shqyrtojë rastin e raportuar me të licencuarin për të vlerësuar:

- Nëse incidenti ka ndodhur për shkak të veprimeve apo mosveprimeve të operatorit,

- Mbi nevojën për rishikimin e akteve rregullatore apo nevojën për mbështetje nga institucionet e tjera ligj zbatuese për veprimet e propozuara me qëllim shmangien, parandalimin apo uljen e numrit të incidenteve.

Në çdo rast ERE mund të kërkojë informacion të detajuar nga OIKI për të mbështetur çdo vlerësim mbi pajtueshmërinë e veprimeve të të licen~~s~~cuarit me rregullat që lidhen me sigurinë e infrastrukturave kritike.

Nëse ERE konkludon se bashkëpunimi me OIKI nuk ka funksionuar ose është e qartë se nuk janë marrë masat e duhura për shmangien e incidenteve në infrastrukturat kritike, ERE do të njoftoj operatorin për dështimet e identifikuara. ERE mund të vendos afate kohore për të korrigjuar dështimet e evidentuara në OIKI.

Neni 9
Penalitetet

Në rast se i licencuari nuk vepron në përputhje me planin e masave, ndaj tij zbatohen sanksione në përputhje me nenin 107 të Ligjit 43/2015 "Për Sektorin e Energjisë Elektrike", nenit 106 të Ligjit Nr. 102/2015 "Për Sektorin e Gazit Natyror" si dhe "Rregulloren për procedurat e vendosjes dhe reduktimit të gjobave" miratuar me vendimin e Bordit të ERE.

Neni 10
Certifikim me standartin e sigurisë ISO 27001

1. Operatorët e Infrastrukturavet Kritike në sektorin e energjisë elektrike dhe gazit natyror të pajisen me certifikimin me standartin e sigurisë ISO 27001 brenda 18 muajve nga hyrja në fuqi e kësaj rregulloreje.
2. Operatorët e Infrastrukturave Kritike të Informacionit, përfshirë Kurum International sh.a, Dragobia Energy, Prell Energy sh.p.k, Power Elektrik Slabinje, Seka Hydropower, Devoll Hydropower sh.a dhe Trans Adriatic Pipeline (TAP), detyrohen të pajisen me certifikimin sipas standardit të sigurisë ISO 27001 brenda 18 muajve nga hyrja në fuqi e këtyre ndryshimeve të rregullores.

~~1.~~3. Operatorët e Infrastrukturave të Rëndësishme të Informacionit, përfshirë Operatorin e Sistemit të Shpërndarjes së Energjisë Elektrike, Termocentralin Vlorë sh.a dhe HEC Vlushe, detyrohen të pajisen me certifikimin sipas standardit të sigurisë ISO 27001 brenda 18 muajve nga hyrja në fuqi e këtyre ndryshimeve të rregullores.

Neni 11
Dispozita përfundimtare

Kjo rregullore hyn në fuqi pas miratimit dhe publikimit të vendimit të Bordit të ERE në fletoren zyrtare.

SHTOJCA1

Raporti i vetëvlerësimit mbi mbrojtjen e infrastrukturave kritike dhe Menaxhimi i Riskut

Operatori bazuar në "Rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë (Miratuar me urdhërin nr. 22, datë 26.04.2018 të ~~AKCESK~~AKSK)" do të raportojë mbi:

Masat Organizative të:

a) menaxhimit të sigurisë së informacionit,
b) menaxhimit të rrezikut,
c) politikave të sigurisë,
ç) sigurisë organizative,
d) kërkesave të sigurisë për palët e treta,
dh) menaxhimit të aseteve,
e) sigurisë së burimeve njerëzore dhe aksesit të personave,
ë) ngjarjeve të sigurisë dhe menaxhimit të incidenteve të sigurisë kibernetike,
f) menaxhimit të vazhdimësisë së punës,
g) kontrollit dhe auditit,

Masat teknike të:

a) sigurisë fizike,
b) mbrojtjes së integritetit të rrjeteve të komunikimit,
c) verifikimit të identitetit të përdoruesve,
ç) menaxhimit për autorizimin e aksesit,
d) veprimtarisë së administratorëve dhe të përdoruesve,
dh) zbulimit të ngjarjeve të sigurisë kibernetike,
e) mjeteve të gjurmimit dhe vlerësimit të ngjarjeve të sigurisë kibernetike,
ë) sigurisë së aplikacioneve,
f) të pajisjeve kriptografike,
g) sigurisë së sistemeve industriale.

SHTOJCA 2

Formulari për raportimin e një incidenti të sigurisë dhe/ose cënimit të integritetit	
Informacion Kontakti	*Emri i Sipërmarrësit:*
	Emri dhe Mbiemri i personit të ngarkuar me eleminimin e incidenteve të sigurisë dhe/ose cënimit të integritetit:
	Pozicioni i Punës:
	Adresa:
	Telefon, e-mail:
Përshkrimi i Incidentit të Sigurisë dhe/ose Cënimit të Integritetit	*Lloji:*
	Përcaktimi se cilat rrjete, sisteme ose shërbime preken nga incidenti i sigurisë:
	Koha e ndodhjes dhe kohëzgjatja:
	Informacion rreth shkakut fillestar ose shkaqeve:
	Përshkrimin e incidentit (përcaktoni të dhënat në mënyrë sa më të detajuar):
	Numri i përafërt i përdoruesve të prekur nga incidenti i sigurisë ose cënimi i integritetit ose përqindja e tyre(%) nga përdoruesit total të rrjetit dhe/ose shërbimit:
	Zona Gjeografike e prekur nga incidenti i sigurisë dhe/ose cënimi i integritetit (km²):
	Burimet e prekura

	Pasojat:
Menaxhimi i incidentit të sigurisë dhe/ose cënimit të integritetit	*Veprimet e ndërmarra (të planifikuara për tu ndërmarrë) për të eleminuar incidentin e sigurisë dhe për të reduktuar pasojat e tij:*
	Masat pas incidentit
Informacione të Tjera të Rëndësishme	*Mësimet e nxjerra*
Data	
Formulari depozitohet pranë Autoritetit Përgjegjës me: *E-mail (të skanuara) në adresën: incidente.raportimi@ere.gov.al*	

SHTOJCA NR.3

Raportimi i vetëvlerësimit të Operatorit mbi impaktin e Incidentit të Sigurisë		
Kohëzgjatja e incidentit të Sigurisë (ndërprerjes së shërbimit, interceptimit të komunikimeve, software të dëmshëm, modifikimi i të dhënave)	*Më tepër se 1 orë, por më pak se 2 orë*	*Më tepër se 2 orë*
Numri i përdoruesve të prekur nga incidenti ose % e tyre ndaj numrit total të përdoruesve		
5%	*Mesatar*	*i Lartë*
Në rast të një numri të panjohur të përdoruesve të prekur nga incidenti i sigurisë do të vlerësohet, zona gjeografike e shtrirjes së incidentit të sigurisë		
➢ **20 km²**		
Vlerësimi Përfundimtar i Impaktit:	**Mesatar**	**i Lartë**