



REPUBLIKA E SHQIPËRISË
KËSHILLI I MINISTRAVE

PROJEKT VENDIM

Nr._____, datë _____.____.2025

**PËR MIRATIMIN E MASAVE PËR SIGURIMIN E
VAZHDUESHMËRISË SË OFRIMIT TË SHËRBIMEVE TË
KOMUNIKIMEVE ELEKTRONIKE NË SITUATA TË
JASHTËZAKONSHME**

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 5, të nenit 174, të ligjit Nr. 54/2024, datë 30.05.2024 “Për komunikimet elektronike në Republikën e Shqipërisë”, me propozimin e zëvendëskryeministrit dhe ministrit për Infrastrukturën dhe Energjinë, Këshilli i Ministrave

V E N D O S I:

1. Miratimin e masave për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve të komunikimeve elektronike në situata të jashtëzakonshme, sipas tekstit që i bashkëlidhet këtij vendimi dhe është pjesë përbërëse e tij.
2. Ngarkohet Ministria e Infrastrukturës dhe Energjisë dhe Autoriteti i Komunikimeve Elektronike dhe Postare për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në “Fletoren Zyrtare”.

KRYEMINISTRI

EDI RAMA

MASAT
PËR SIGURIMIN E VAZHDUESHMËRISË SË OFRIMIT TË
SHËRBIMEVE TË KOMUNIKIMEVE ELEKTRONIKE NË SITUATA
TË JASHTËZAKONSHME

Neni 1
Qëllimi

1. Ky vendim përcakton masat për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve të komunikimeve elektronike me qëllim përballimin e situatave të jashtëzakonshme duke:
 - a) minimizuar ndikimin e situatave të jashtëzakonshme në marrjen e shërbimeve të komunikimeve nga përdoruesit e rrjeteve të komunikimeve elektronike;
 - b) siguruar rikuperimin e shpejtë dhe të sigurt të funksioneve kritike të komunikimeve pas një ndërprerjeje të mundshme dhe
 - c) siguruar pajtueshmërinë me kërkesat ligjore për sigurinë dhe integritetin e rrjeteve të komunikimeve elektronike në situata të jashtëzakonshme.
2. Ky vendim ka për qëllim sigurimin e bashkërendimit të masave dhe bashkëpunimit për përballimin e situatave të jashtëzakonshme në rrjetet dhe shërbimet e komunikimeve elektronike në Republikën e Shqipërisë.

Neni 2
Fusha e zbatimit

Ky vendim zbatohet për sipërmarrësit e komunikimeve elektronike të autorizuar nga Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP) për ofrimin e rrjeteve dhe shërbimeve të komunikimeve elektronike, bazuar në ligjin nr. 54/2024, datë 30.05.2024 “Për komunikimet elektronike në Republikën e Shqipërisë”.

Neni 3
Përkufizime

Përveç përkufizimeve të dhëna në nenin 4, të ligjit nr. 54/2024, “Për komunikimet elektronike në Republikën e Shqipërisë”, për qëllime të këtij dokumenti, termat e mëposhtëm kanë këto kuptime:

- a) “Situatë e jashtëzakonshme” nënkupton dëmtimet e rënda të rrjetit të komunikimeve elektronike, fatkeqësitë natyrore, gjendjen e emergjencës civile sipas përcaktimeve në ligjin për emergjencat civile ose gjendjen e luftës.

- b) “Komiteti Ndërmintor i Emergjencave Civile (KNEC)” është një organ i përkohshëm, që krijohet menjëherë pas shpalljes së gjendjes së fatkeqësisë natyrore sipas përcaktimeve në ligjin për emergjencat civile.
- c) “Agjencia Kombëtare e Mbrojtjes Civile (AKMC)”, është agjencia në varësi të ministrit përgjegjës për mbrojtjen civile që vepron sipas përcaktimeve në ligjin për emergjencat civile.
- d) “AKSK”, është Autoriteti Kombëtar për Sigurinë Kibernetike, organi publik përgjegjës për zbatimin dhe mbikëqyrjen e ligjit për sigurinë kibernetike.

Neni 4

Detyrimet e sipërmarrësve të komunikimeve elektronike

1. Në zbatim të parashikimeve të nenit 174, të ligjit nr. 54/2024, “Për komunikimet elektronike në Republikën e Shqipërisë”, sipërmarrësit e komunikimeve elektronike hartojnë dhe paraqesin në AKEP planin e masave për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve, sipas përcaktimeve në këtë vendim.
2. Në situatat e jashtëzakonshme sipërmarrësit e komunikimeve elektronike bashkëpunojnë me Ministrinë përgjegjëse për komunikimet elektronike dhe AKEP me qëllim zbatimin e masave të emergjencës dhe koordinimin me:
 - a) Komitetin Ndërmintor të Emergjencave Civile (KNEC)
 - b) Komitetin e Mbrojtjes Civile (KMC)
 - c) Agjencinë Kombëtare të Mbrojtjes Civile si dhe
 - d) Autoritetet, strukturat e tjera përgjegjëse të ngritura në rastet e emergjencave kombëtare në përputhje me legjislacionin në fuqi.
3. Në rastin e sulmeve kibernetike, sipërmarrësit e komunikimeve elektronike bashkëpunojnë me AKEP dhe AKSK sipas parashikimeve ligjore për sigurinë kibernetike dhe rregullat për sigurinë dhe integritetin e rrjeteve sipas ligjit për komunikimet elektronike.

Neni 5

Plani i masave për sigurimin e vazhdueshmërisë së shërbimeve

1. Për menaxhimin e vazhdimësisë së punës sipërmarrësit e komunikimeve elektronike krijojnë dhe mbajnë plane emergjence dhe një strategji për të siguruar vazhdimësinë e rrjeteve të komunikimit dhe sistemeve të informacionit.
2. Plani i masave për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve dhe mirëfunksionimin e infrastrukturës së tyre në rastet e jashtëzakonshme që hartohet nga sipërmarrësi i komunikimeve elektronike përmban minimalisht parashikimet si më poshtë:
 - a) përcaktimin e qëllimit dhe fushëveprimit të planit të masave;
 - b) përcaktimin e objektivave të planit;
 - c) përcaktimin e strukturave përgjegjëse organizative si:

- i. ekipin e menaxhimit të krizës;
 - ii. ekipin e vlerësimit të dëmtimeve
 - iii. ekipin e mbështetjes teknike që zbaton procedurat teknike të rikuperimit;
 - iv. ekipin e komunikimit;
 - v. ekipin e sigurisë së informacionit.
 - d) përgjegjësitë e strukturave përkatëse për situatat e jashtëzakonshme;
 - e) procesin e analizimit dhe identifikimit të sistemeve kritike
 - f) strategjitë e Backup-it dhe Ruajtjes së të dhënave
 - g) infrastrukturën e rikuperimit
 - h) procedurat e rikuperimit
 - i) planin e komunikimit dhe koordinimit
 - j) testimin dhe mirëmbajtjen e planit
 - k) aspektet ligjore, përputhshmërinë me standardet e sigurisë, reagimit në situata të emergjencave;
 - l) trajnimin dhe ndërgjegjësimin e stafit;
 - m) rishikimin periodik të planit.
3. Një model orientues për hartimin e planit të masave nga sipërmarrësit jepet në aneksin 1, bashkëlidhur këtij vendimi.

Neni 6

Masat për sigurimin e vazhdueshmërisë së ofrimit të shërbimit

1. Masat për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve të komunikimeve elektronike në situata të jashtëzakonshme përfshijnë:
 - a) Masat parandaluese, përgatitore për situata të jashtëzakonshme;
 - b) Masat gjatë situatës së jashtëzakonshme;
 - c) Masat e rikuperimit.
2. Masat për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve përfshijnë gjithashtu masat parandaluese, të vazhdimësisë dhe rikuperimit në rastin e sulmeve kibernetike. Lista e masave dhe kërkesat për dokumentimin e tyre jepen në aneksin 2, bashkëlidhur këtij vendimi.

Neni 7

Masat parandaluese

1. Sipërmarrësit e komunikimeve elektronike hartojnë dhe të mirëmbajnë:
 - a) Planin e vazhdimësisë së biznesit (Business Continuity Plan – BCP);
 - b) Planin e rikuperimit pas fatkeqësisë (Disaster Recovery Plan – DRP).
2. Sipërmarrësit e komunikimeve elektronike identifikojnë dhe raportojnë pranë AKEP, asetet dhe burimet kritike të rrjetit si dhe pajisjet e lëvizshme që disponojnë me sigurimin e vazhdueshmërisë së ofrimit të shërbimit në raste të jashtëzakonshme brenda 3 (tre) muajve nga hyrja në fuqi e këtij vendimi.

3. Me qëllim sigurimin e vazhdimësisë së ofrimit të shërbimeve në situatë të jashtëzakonshme, sipërmarrësit e komunikimeve elektronike zbatojnë standardet e sigurisë duke marrë masa:
 - a) për instalimin e linjave rezervë, serverë pasivë, mjete komunikimi të bazuara në teknologji cloud dhe lidhje të pavarura për stacionet bazë dhe shërbimet kritike.
 - b) pajisin qendrat e të dhënave, stacionet dhe antenat transmetuese me burime alternative të furnizimit me energji;
 - c) sigurojnë funksionalitetin e shërbimeve të emergjencës, dhe numrit 112 edhe pa kartë SIM.
4. Sipërmarrësit duhet të marrin pjesë dhe bashkëpunojnë me autoritetet përgjegjëse në ushtrimet kombëtare të simulimit të organizuara.
5. Operatorët duhet të caktojnë një person kontakti për 24 orë/7 ditë gjatë situatave të jashtëzakonshme duke përditësuar të dhënat e kontaktit në AKEP.

Neni 8

Masat e reagimit gjatë emergjencës

1. Në rastin e situatave të jashtëzakonshme, sipërmarrësit e komunikimeve elektronike, aktivizojnë menjëherë ekipet e brendshme të menaxhimit të krizës, situatat e emergjencës dhe njoftojnë pa vonesë AKEP për çdo ndërprerje të shërbimeve.
2. Sipërmarrësit duhet të aktivizojnë kanale prioritare për komunikimin e institucioneve shtetërore dhe sipas rastit vendosin në operim pajisjet lëvizëse të rrjetit për mbulimin me shërbim si dhe sigurojnë transmetimin e paralajmërimeve publike për emergjencat civile apo fatkeqësitë e mëdha në zhvillim ose të pritshme, drejt përdoruesve fundorë të prekur përkatësisht.
3. Aktivizojnë burimet alternative të energjisë për qendrat e të dhënave, stacionet dhe antenat transmetuese.
4. Përdorin ri-rrugëzimin automatik të lidhjeve përmes lidhjeve rezervë, përfshirë dhe ato ndërkombëtare. Përdorimi i sistemeve satelitore për mbulimin me sisteme komunikimi për autoritetet.
5. Sigurojnë akses për përdoruesit në shërbimet bazë të emergjencës.
6. Gjatë krizës, situatës së jashtëzakonshme, raportojnë çdo 4 orë pranë ministrisë përgjegjëse dhe AKEP-it.

Neni 9

Masat e rikuperimit pas emergjencës

1. Sipërmarrësit e komunikimeve elektronike bëjnë vlerësimin dhe raportojnë në AKEP për dëmet brenda 48 orëve pas ngjarjes.
2. Sipërmarrësit e komunikimeve elektronike duhet të rikthejnë funksionalitetin e rrjetit në përputhje me planin e rikuperimit, sipas nenit 7, të këtij vendimi.

3. Sipërmarrësit e komunikimeve elektronike duhet të kryejnë një analizë pas ngjarjes me AKEP dhe institucionet e sigurisë.
4. Sipërmarrësit e komunikimeve elektronike duhet të përditësojnë planet BCP/DRP dhe të raportojnë tek AKEP.
5. Sipërmarrësit e komunikimeve elektronike ndërtojnë një manual praktik për përmirësim të kapaciteteve reaguese në të ardhmen.

Neni 10

Masat për sigurinë në rastet e sulmeve kibernetike

1. Pa anashkaluar zbatimin e masave sipas parashikimeve në nenin 20 të ligjit nr. 25/2024 “Për Sigurinë Kibernetike”, si dhe në nenin 54 dhe 157 të ligjit Nr. 54/2024 “Për komunikimet elektronike në Republikën e Shqipërisë”, në kuadër të masave për të realizuar sigurinë e rrjeteve dhe shërbimeve, me qëllim përballim e situatave në rastet e sulmeve kibernetike, sipërmarrësit e komunikimeve elektronike marrin masat si më poshtë:
 - a) të kryejnë vlerësime periodike të rrezikut kibernetik çdo 12 muaj.
 - b) të kenë në funksionim sisteme të monitorimit dhe analizës (SIEM/SOC) për detektimin e anomalive.
 - c) të zbatojnë arkitekturën “*Zero Trust*”, me akses të kufizuar sipas funksioneve.
 - d) të mbajnë kopje rezervë offline të sistemeve dhe konfigurimeve kritike.
 - e) të kryejnë testime dhe simulime për skenarë emergjencash kibernetike.
 - f) të kenë një plan të shkruar të reagimit ndaj incidenteve (IRP), të certifikuar nga AKSK.
2. Sipërmarrësit e komunikimeve elektronike, njoftojnë brenda afateve ligjore AKSK dhe AKEP për incidentin kibernetik.
3. Sipërmarrësit e komunikimeve elektronike aktivizojnë kanale të sigurta të komunikimit me autoritetet dhe duhet të realizojnë kriptimin e detyrueshëm të të gjitha lidhjeve të transmetimit.
4. Në rastin e incidenteve të kryejnë izolimin e pjesëve të komprometuara të rrjetit, respektojnë standardet e sigurisë për kontrollin e aksesit si dhe kryejnë auditim dhe analizë të plotë teknike të incidentit.
5. Sipërmarrësit e komunikimeve elektronike hartojnë raportin e incidentit dhe e paraqesin në AKEP dhe AKSK brenda afatit të përcaktuar.
6. Sipërmarrësit e komunikimeve elektronike rishikojnë periodikisht politikat e brendshme të sigurisë, planet e vazhdimësisë së biznesit dhe planet e reagimit ndaj incidenteve, si dhe kryejnë rregullisht trajnimin e stafit për sigurinë kibernetike.

Neni 11

Bashkëpunimi ndërkombëtar

Në rastet e jashtëzakonshme dhe sipas nevojës, bazuar në Konventën Tampere dhe marrëveshjet e bashkëpunimit ku Shqipëria është palë, ministria përgjegjëse për komunikimet elektronike dhe AKEP, në bashkëpunim me autoritetet përgjegjëse mund të kërkojnë ndihmë nga partneret ndërkombëtare, vendet pjesëmarrëse në Konventën Tampere, për sigurimin e pajisjeve të komunikimit të lëvizshme, përfshirë mbulimin me komunikime satelitore me qëllim sigurimin e shërbimeve të telekomunikacionit sipas përcaktimeve në Konventën Tampere.

Neni 12

Autorizimet e përkohshme për rastet e emergjencave

Me qëllim përballimin e situatave të emergjencave, AKEP sipas parashikimeve në ligjin për komunikimet elektronike dhe Planin Kombëtar të Frekuencave, ka të drejtë të japë autorizime të përkohshme për përdorimin e frekuencave rezervë për rastet e emergjencave me qëllim sigurimin e komunikimeve elektronike. Operatorët që veprojnë në fushën e ndihmës ndërkombëtare në rastin e marrjes së ndihmës përmes Konventës Tampere parashikuar në nenin 11, mund të pajisen me autorizim të përkohshëm për përdorimin e pajisjeve dhe frekuencave, sipas një procedure të përshpejtuar.

Neni 13

Koordinimi operacional dhe pika kombëtare e kontaktit

Në rastin e situatave të jashtëzakonshme, me qëllim koordinimin e veprimeve për sigurimin e shërbimeve të komunikimeve elektronike, pranë ministrisë përgjegjëse krijohet njësi e koordinimit që bashkëpunon me AKEP dhe autoritetet përgjegjëse për emergjencat me qëllim koordinimin e veprimeve për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve të komunikimit. Ministria cakton një pikë kombëtare kontakti për të koordinuar me ITU, autoritetet përgjegjëse për emergjencat dhe partnerët ndërkombëtarë për të kërkuar ndihmë sipas nenit 11, në zbatim të Konventës Tampere.

Neni 14

Regjistri i operatorëve dhe shërbimeve të autorizuar

AKEP mbi bazën e informacioneve të sipërmarrësve dhe në bashkëpunim me ministrinë përgjegjëse për komunikimet elektronike krijon një regjistër të sipërmarrësve që zotërojnë pajisje të lëvizshme telekomunikacioni që mund të perdoren për rastet e emergjencave.

Neni 15

Testimet dhe auditimet

Sipërmarrësit e komunikimeve elektronike organizojnë të paktën 1 (një) herë në vit teste ose simulime të kapaciteteve të telekomunikacionit në raste emergjente. Testimet dhe auditimet duhet të jenë të dokumentuara. Testimet dhe auditimet kryhen dhe me kërkesë e prezencë të përfaqësuesve të AKEP dhe/ose të Ministrisë/autoriteteve përgjegjëse.

Neni 16

Mbrojtja e të dhënave dhe proporcionaliteti

Veprimtaritë sipas këtij vendimi kryhen në përputhje me ligjin nr.124/2024 “Për mbrojtjen e të dhënave personale” dhe kufizohen vetëm në masat e domosdoshme, të nevojshme dhe proporcionale për arritjen e qëllimeve të këtij vendimi.

Neni 17

Përgjegjësia dhe sanksionet

Në rast mosrespektimi të kërkesave të këtij vendimi për hartimin e planit të masave për vazhdueshmërinë e ofrimit të shërbimit në raste të jashtëzakonshme, AKEP ndërmerr masat administrative në përputhje me parashikimet e ligjit nr. 54/2024 për vendosjen e gjobave. Në raste të përsëritura ose refuzim të qëllimshëm, AKEP mund të kërkojë pezullimin e përkohshëm të aktivitetit, revokimin e autorizimeve përkatëse.

Neni 18

Hyrja në fuqi

Ky vendim hyn në fuqi pas botimit në “Fletoren Zyrtare”.

Model orientues për sipërmarrësit për Planin e Masave

Plani i Masave për Vazhdueshmërinë e Ofrimit të Shërbimeve të komunikimeve elektronike në raste të jashtëzakonshme

Për: _____

Sektori: Telekomunikacion/komunikimeve elektronike

1. Qëllimi dhe Fushëveprimi

Ky dokument përcakton politikat, procedurat dhe përgjegjësitë për rikuperimin e sistemeve kritike të rrjetit dhe shërbimeve të komunikimeve të _____ në rast fatkeqësie ose ndërprerjeje të rëndë. Plani zbatohet për të gjitha sistemet, rrjetet dhe qendrat e të dhënave të operatorit që ndikojnë në ofrimin e shërbimeve të komunikimit elektronik për klientët.

2. Objektivat e Planit

- Sigurimi i rikuperimit të shpejtë dhe të sigurt të funksioneve kritike pas një ndërprerjeje.
- Minimizimin e ndikimit ndaj përdoruesve (individë, biznes, autoritete publike) dhe infrastrukturës kombëtare të komunikimit.
- Pajtueshmëria me kërkesat ligjore për sigurinë dhe me kërkesat kombëtare për vazhdimësinë e shërbimit.

3. Struktura Organizative dhe Përgjegjësitë

Ekipet përgjegjëse për zbatimin e DRP përfshijnë:

- Ekipi i Menaxhimit të Krizës – koordinon përgjigjen e përgjithshme ndaj incidentit.
- Ekipi i Teknik, operimit dhe mirëmbajtjes së Rrjetit – zbaton procedurat teknike të rikuperimit.
- Ekipi i vleresimit të demtimeve
- Ekipi i Komunikimit – menaxhon njoftimet publike dhe komunikimin me autoritetet.
- Ekipi i Sigurisë së Informacionit – monitoron aspektet e sigurisë kibernetike gjatë rikuperimit.

4. Analiza e Sistemeve kritike

Operatori _____, identifikon sistemet dhe shërbimet kritike që kanë ndikim të drejtpërdrejtë në funksionimin e rrjetit kombëtar të telekomunikacionit, duke përcaktuar për secilin:

- Objektivat për kohën maksimale e pranueshme për rikuperim;
- Objektivat për kufiri maksimal i humbjes së të dhënave të pranueshme.

5. Strategjite e Backup-it dhe Ruajtjes së të dhënave

- Backup-et kryhen çdo ditë për sistemet kritike dhe ruhen në një lokacion off-site të sigurt.
- Kopjet e të dhënave ruhen në cloud dhe në një qendër alternative të të dhënave (hot site).
- Integriteti i backup-eve testohet periodikisht për të garantuar rikthimin e plotë të të dhënave.

6. Infrastruktura e Rikuperimit

Operatori _____ mban kapacitete alternative operative për rikuperimin e shërbimeve:

- Qendër rezervë me pajisje të gatshme për aktivizim të menjëhershëm;
- Kapacitete të përgatitura pjesërisht për aktivizim brenda 24 orëve
- Cold Site – Ambient rezervë pa pajisje, për raste ekstreme.

7. Procedurat e Rikuperimit

Në rast fatkeqësie, aktivizohen procedurat e mëposhtme:

1. Vlerësimi i incidentit dhe njoftimi i menjëhershëm i Ekipit të Menaxhimit të Krizës.
2. Aktivizimi i qendrës rezervë dhe rikthimi i serverëve kritikë.
3. Rikthimi i bazave të të dhënave dhe lidhjeve të rrjetit.
4. Testimi i funksionimit të plotë para rifillimit të shërbimeve për publikun.

8. Plani i Komunikimit dhe Koordinimi

Operatori X mban linja të dedikuara komunikimi për situata emergjente dhe një plan komunikimi të krizës që përfshin:

- Informimin e autoriteteve rregullatore (AKEP, AKSK);
- Komunikimin me klientët dhe partnerët për ndërprerjet;
- Përdorimin e kanaleve alternative të komunikimit në rast dështimi të rrjeteve primare.

9. Testimi dhe Mirembajtja e Planit

Plani testohet të paktën dy herë në vit përmes simulimeve dhe ushtrimeve praktike. Pas çdo testi ose incidenti real, plani përditësohet në bazë të mësimave të nxjerra. Verifikimet përputhen me kërkesat e NIS2 dhe udhëzimet e ENISA për testimin e qëndrueshmërisë së rrjeteve.

10. Aspektet ligjore dhe përputhshmeria

Ky plan është në përputhje me përcaktimet e ligjit për komunikimet elektronike dhe ligjit për emergjencat civile, ligjit për sigurinë kibernetike, dhe rregulloret përkatëse të AKEP. Operatorët janë të detyruar të raportojnë incidentet madhore të sigurisë brenda 24 orëve nga identifikimi i tyre dhe të bashkëpunojnë me autoritetet për rikuperim të plotë.

11. Trajnimi dhe ndërgjegjësimi

Të gjithë punonjësit e përfshirë në zbatimin e DRP-së trajnohen periodikisht mbi procedurat e reagimit, sigurisë së informacionit dhe komunikimit në situata emergjente. Operator X organizon ushtrime praktike dhe verifikon gatishmërinë e personelit në çdo nivel.

Ky plan hyn në fuqi më datë: _____ dhe rishikohet çdo 12 muaj.

MASAT PËR SIGURIMIN E VAZHDUESHMËRISË SE SHËRBIMEVE PARA, GJATË DHE MBAS SITUATAVE TË JASHTËZAKONSHME DHE DOKUMENTIMI

Masat e sigurisë	Dokumentacioni
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të implementojë një strategji për vazhdimësinë e ofrimit të shërbimit për rrjetet e komunikimit dhe sistemet e informacionit.	Strategjia/Plani i dokumentuar për vazhdimësinë e shërbimit, duke përfshirë kohën e rikuperimit për shërbimet dhe proceset kryesore. Dokumentim i “ <i>Business Continuity Plan</i> ” (BCP);
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të implementojë dhe zbatojë planet e emergjencës për sektoret dhe shërbimet kritike.	Planet e emergjencës për sistemet kritike duke përfshirë hapa të qarta dhe procedurat për kërcënimet e njohura, shkaktuesit për aktivizimin, hapat dhe kohën e rikuperimit. Dokumentimi “ <i>Disaster Recovery Plan</i> ” (DRP).
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të monitorojë aktivitetet dhe zbatimin e planeve të emergjencës, regjistrimi i tentativave të suksesshme të rikuperimit dhe dështimet	Dokumentimi që identifikon asetet dhe nyjet kritike të rrjetit.
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të kryejë rishikimin dhe kontrollin periodik të strategjisë për vazhdimësinë e shërbimit	Dokumentimi që tregon që sipërmarrësi ka linja rezervë, serverë pasivë, mjete komunikimi të bazuara në teknologji cloud dhe lidhje të pavarura për stacionet bazë dhe shërbimet kritike.
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të testohjë planet rezervë(backup) dhe të emergjencës për të siguruar që sistemet dhe proceset funksionojnë dhe që personeli është i përgatitur në rastin e dëmtimeve të mëdha dhe emergjencave.	Dokumentimi që tregon që sipërmarrësi ka pajisur qendrat e të dhënave, stacionet dhe antenat transmetuese me burime alternative të energjisë.
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të implementojë një program për ushtrimin rregullisht të planeve rezervë dhe të emergjencës, duke përdorur skenarë realistë që mbulojnë një sërë skenarësh të ndryshëm me kalimin e kohës.	Dokumentimi që garanton funksionalitetin e numrin unik evropian të emergjencave “112” edhe pa kartë SIM si dhe dhe çdo numër kombëtar të emergjencës, të përcaktuar sipas legjislacionit në fuqi.
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të rishikojë dhe përditësojë planet duke marrë në konsideratë ndryshimet, incidentet e mëparshme dhe emergjencat që nuk kanë qenë të mbuluara nga programi i ushtrimit.	Dokumentimi që tregon që sipërmarrësi ka marrë pjesë në ushtrime kombëtare simulimi të organizuara nga AKEP dhe institucionet përgjegjëse.
- Përfshirja në ushtrime e furnitorëve dhe palëve të tjera të treta. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të rishikojë dhe përditësojë planet duke marrë në konsideratë ndryshimet, incidentet e mëparshme dhe emergjencat që nuk kanë qenë të mbuluara nga programi i ushtrimit. - Mësimet e nxjerra nga këto ushtrime të jenë adresuar nga personat përgjegjës dhe në përputhje me rrethanat të bëhet përditësimi i proceseve dhe sistemeve përkatëse.	Dokumentimi që tregon që sipërmarrësi ka caktuar person kontakti në raste të jashtëzakonshme që komunikon me AKEP.
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të	Dokumentimi i aktivizimit dhe zbatimit të planeve të emergjencës, duke përfshirë vendimet e marra, hapat e ndjekur, kohën e plotë të rikuperimit. Dokumentacion që sipërmarrësi ka

përgatiten për rikthimin në gjendjen normale të sistemeve të komunikimeve elektronike. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të implementojë politika/procedura për vendosjen e kapaciteteve për rikuperimin e infrastrukturave të komunikimit elektronike.	parashikuar ngritjen e qendrës së reagimit të emergjencave ose ekipit/eve të brendshëm të emergjencës.
	Dokumentacioni që sipërmarrësi ka përcaktuar sistemin njoftimi për autoritetet përkatëse për çdo ndërprerje të shërbimeve.
	Dokumentacioni që sipërmarrësi ka ose siguruar mjete të lëvizshme të rrjetit telefonik celular për t'u vendosur në terren.
	Dokumentimi që tregon që sipërmarrësi ka pajisur qendrat e të dhënave, stacionet dhe antenat transmetuese me burime alternative energjie.
	Dokumentacioni që sipërmarrësi ka në përdorin ri-rutim automatik të lidhjeve përmes lidhjeve rezervë, përfshirë dhe ato ndërkombëtare. Përdorimi i sistemeve satelitore për mbulimin me sisteme komunikimi për autoritetet.
	Dokumentacioni që sipërmarrësi ka siguruar akses për përdoruesit në shërbimet bazë emergjente (telefoni, 112, SMS).
	Dokumentacioni që sipërmarrësi ka raportuar gjatë krizës drejt AKEP-it dhe strukturave të tjera gjatë situatës
	Strategjia e përditësuar e vazhdimësisë dhe planet e emergjencës, shqyrtimi i komenteve dhe/ose ndryshimi i logeve. Dokumentacioni që sipërmarrësi ka bërë vlerësim dhe raportim për dëmet brenda 48 orëve pas ngjarjes.
	Dokumentacioni që sipërmarrësi ka rikthyer funksionalitetin e rrjetit dhe shërbimeve sipas planit të rikuperimit.
	Dokumentacioni që sipërmarrësi ka kryer një analizë pas ngjarjes dhe ka raportuar me AKEP dhe institucionet e përcaktuara me ligj..
	Dokumentacioni që sipërmarrësi ka përditësuar planet BCP/DRP dhe ka raportuar tek AKEP.
	Dokumentacioni që sipërmarrësi ka ndërtuar një manual praktik për përmirësim të kapaciteteve reaguese në të ardhmen.

MASAT PËR VAZHDUESHMËRINË E OFRIMIT TË SHËRBIMEVE NË RASTIN E SULMEVE KIBERNETIKE

Masat	Dokumentacioni
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike ose të shërbimeve të komunikimeve elektronike merr masat e duhura teknike, organizative dhe proporcionale për të menaxhuar në mënyrë të përshtatshme rreziqet që vijnë për sigurinë e rrjeteve dhe shërbimeve. Implementimi i monitorimit të logeve për sistemet e informacionit - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të kryejë rishikime menaxheriale të menaxhimit të sigurisë së sistemeve, logeve dhe raporteve të monitorimit të rrjeteve të komunikimit dhe të sistemeve të informacionit. - Implementimi i politikavë të ngjarjeve dhe monitorimit të sistemeve - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të rishikojë dhe përditësojë politikat dhe procedurat duke marrë parasysh ndryshimet dhe incidentet e mëparshme.	Dokumentimi që tregon që sipërmarrësi ka kryer vlerësime të rrezikut kibernetik çdo 12 muaj.
	Dokumentimi që tregon që sipërmarrësi ka në funksionim sisteme të monitorimit dhe analizës (SIEM/SOC) për detektimin e anomalive.
	Dokumentimi që tregon që sipërmarrësi ka zbatuar arkitekturën Zero Trust, me akses të kufizuar sipas funksioneve.
	Dokumentimi që tregon që sipërmarrësi ka kopje rezervë offline të sistemeve dhe konfigurimeve kritike.
	Dokumentimi që tregon që sipërmarrësi ka kryer testime dhe simulime për skenarë emergjencash kibernetike.
	Dokumentimi që tregon që sipërmarrësi ka një plan të shkruar të reagimit ndaj incidenteve (IRP), të certifikuar nga AKSK.
	Dokumentimi që tregon që sipërmarrësi ka sisteme njoftimi për institucionet e AKSK dhe AKEP në rast incidenti.
	Dokumentimi që tregon që sipërmarrësi ka aktivizuar kanale të sigurta të komunikimit me autoritetet.
	Dokumentimi që tregon që sipërmarrësi ka kryer izolimin e pjesëve të komprometuara të rrjetit dhe kontrollin e aksesit.
	Dokumentimi që tregon që sipërmarrësi ka kryer auditim forensik dhe analizë e plotë teknike të incidenteve.
	Dokumentimi që tregon që sipërmarrësi ka hartuar raportin e incidentit dhe ka dorëzuar te AKEP dhe AKSK.
	Dokumentimi që tregon që sipërmarrësi ka rishikuar politikat e brendshme të sigurisë dhe trajnimit të stafit.
	Dokumentimi që tregon që sipërmarrësi ka përditësuar planet e vazhdimësisë së biznesit (BCP) dhe reagimit ndaj incidenteve (IRP).