REPUBLIKA E SHQIPËRISË

AUTORITETI I KOMUNIKIMEVE ELEKTRONIKE DHE POSTARE

RREGULLORE

Nr___datë 10.07.2015

MBI MASAT TEKNIKE DHE ORGANIZATIVE PER TE GARANTUAR SIGURINE DHE INTEGRITETIN E RRJETEVE DHE/OSE SHERBIMEVE TE KOMUNIKIMEVE ELEKTRONIKE[1]

Miratuar me Vendim të Këshillit Drejtues të AKEP nr.2592datë 10.07.2015

[1] Kjo Rregullore perafron Nenin 13 a) Kapitulli III a), të ***Direktivës Kuadër 2002/21/EC*** amenduar me Direktivën 2009/140/EC e Parlamentit European dhe Këshillit; Nenin 4 të ***Direktivës e-Privacy 2002/58/EC*** amenduar me Direktivën 2009/136/EC të Parlamentit Europian dhe Këshillit datë 25.11.2009 si dhe rregullat nga manualet guidë të ENISA.

Neni 1

Dispozita të përgjithshme

Kjo Rregullore është hartuar në përputhje te Nenit 6, gërma p) e nenit 8, nenit 122 të Ligjit nr.9918, datë 19. 05. 2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar ***(ligji nr. 9918/2008***).

Neni 2

Përkufizime

Përvec sa parashikohet në Ligjin nr.9918, datë 19. 05. 2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar ***(ligji nr. 9918/2008***), termat e meposhtëm do të kenë këto kuptime:

1. **"Incidenti i Sigurise"** do te thote Një shkelje e sigurisë ose një humbje e integritetit që mund të ketë një ndikim në funksionimin e rrjeteve dhe sherbimeve të komunikimeve elektronike dhe shërbimeve.

2. **"Asetet e infrastruktures"** do te thote: Të gjitha pjeset e infrastruktures te ofruesit te sherbimeve te cilave, kur u cenohet dhe / ose dështojne, mund të kene një ndikim negativ në sigurinë apo vazhdimësinë e sherbimeve dhe rrjeteve të komunikimit elektronik apo shërbimeve.
3. **"Mohimi i Sherbimit -Denial of Service (DoS)" -** do te thote veprimet, te cilat interferojne me punen e rrjeteve te komunikimit publik dhe /ose sistemeve te informacionit duke sjelle si pasoje mungese te sherbimeve per nje periudhe kohore.

4. **"Kompromentimi i Sistemeve te Informacionit"** do te thote perdorimi i jashteligjshem i burimeve te sistemeve te informacionit dhe/ose aksesi i pa autorizuar ne keto sisteme.

5. **"Software i Demshem (Malicious Software)"** do te thote nje softëare i plote ose nje pjese e tij e dizenjuar per tu lidhur me ose per te mundesuar aksesin e pa autorizuar ne sistemin e informacionit ose ne nje rrjet te komunikimit publik, modifikimin e operacioneve te sistemit te informacionit ose rrjetit te komunikimit publik, shkaterrimin, demtimin, fshirjen ose ndryshimin e te dhenave elektronike, eleminimin ose kufizimin e mundesise se perdorimit te te dhenave elektronike, qe con ne pervetesim ose perdorim te te dhenave elektronike jo publike nga njerezit, qe nuk kane te drejtat per te kryer kete gje.

6. **"Manipulimi i te Dhenave Elektronike"** do te thote shperdorimi dhe me tej perhapja dhe publikimi i te dhenave elektronike, zevendesimi i tyre me te dhena te tjere elektronike, deformimi i te dhenave elektronike ose cdo perdorimin tjeter i jashteligjshem i tyre.

Neni 3

Qellimi

Kjo rregullore percakton detyrimin e operatoreve që operojne nën regjimin e Autorizimit të Përgjithshem për ofrimin e rrjeteve dhe/ose shërbimeve publike të komunikimeve elektronike, që të marrin masat e duhura gjatë projektimit, instalimit dhe funksionimit të rrjetit ose pajisjeve të perdorura, në mënyrë që të garantojnë sigurinë, integritetin dhe funksionimin e rrjeteve të komunikimit elektronike, si dhe te paraqesin prane AKEP, sipas Aneks nr.1 dhe Aneks nr.2, cdo nderhyrje, cenim ose incident ne sigurine dhe integritetin e rrjeteve te komunikimit elektronik publik qe ka nje impakt te konsiderueshem ne funksionimin e rrjeteve dhe/ose te sherbimeve te tyre

Neni 4

Objekti

Kjo Rregullore synon:

a) Te percaktoje objektivat dhe masat per garantimin e funksionimit të infrastrukturës se rrjetit dhe/ose sherbimeve te komunikimit elektronik nga operatoret qe ofrojne akses ne rrjetet e komunikimit publik dhe /ose ne sherbimet e komunikimit publik, ne respekt te konfidencialitetit, integritetit dhe ofrimit te panderprere te sherbimeve.

b) Te percaktoje detyrimet dhe masat baze qe operatoret duhet te ndermarrin per te minimizuar apo parandaluar ndodhjen e incidenteve te sigurise ne rrjetet dhe/ose sherbimet e komunikimeve elektronike, dhe per ti raportuar ato nese ndodhin.

c) Kushtet qe duhet te plotesoje nje cenim ose incident sigurie, ne menyre qe te linde detyrimi i operatoreve per te informuar AKEP ne lidhje me kete cenim ose incident sigurie.

d) Standardizimi në vleresimin dhe raportimin e masave te sigurise te ndermarra nga operatoret dhe te incidenteve te sigurise.

e) Menyren dhe permbajtjen e raportimit te masave te sigurise dhe incidenteve te sigurise qe duhet dorezuar ne AKEP.

f) Percaktimi i sanksioneve, masave administrative ne rast se operatoret deshtojne ne permbushjen e detyrimeve te percaktuara ne kete rregullore.

Neni5

Fusha e zbatimit e Rregullores

Percaktimet e kesaj rregulloreje jane te detyrueshme per tu zbatuar nga te gjithe operatoret e autorizuar nga AKEP të cilët ofrojne akses ne rrjetet apo sherbimet (fushen) e komunikimeve elektronike publike në përputhje me legjislacionin në fuqi.

Neni 6

Detyrimet e Operatoreve

1. Operatoret duhet te informojne AKEP brenda 3 ditëve, cdo here qe ndodh nje nga incidentet e meposhtme te sigurise:
   - Mohimi i Sherbimeve Elektronike
   - Kompromentimi i Sistemeve te Informacionit
   - Manipulimi ose modifikimi i paautorizuar i te Dhenave Elektronike
   - Softëare te demshem (spam, virus, spyëare etj)

2. Operatoret duhet te informojne AKEP menjehere rreth incidenteve te zbuluara te sigurise dhe/ose Cenimit te Integritetit, te cilat kane pasur, kane ose mendohet se do te kene nje impakt te rendesishem dhe / ose mesatar ne ofrimin e rrjeteve te komunikimit publik dhe/ose ne sherbimet e komunikimit elektronik publik te perdoruesit.

3. Operatoret duhet te implementojne mjetet dhe metodat e duhura teknike dhe organizative per te garantuar sigurine e rrjeteve te komunikimit publik dhe te sherbimeve te ofruara prej tyre. Keto mjete duhet te sigurojne nivelin e sigurise ne perputhje me rrezikun e paraqitur dhe te evitojne incidentet e sigurise nga ndodhja e tyre ose te reduktojne impaktin ose pasojat kur keto incidente ndodhin.

4. Operatoret duhet te implementojne mjetet e duhura teknike dhe organizative per te garantuar integritetin e rrjeteve te komunikimit publik, duke siguruar ne kete menyre ofrimin e panderprere te sherbimeve te tyre.

5. Operatoret duhet te menaxhojne dhe mbrojne mjedisin dhe pajisjet e perdorura per ofrimin e rrjeteve te komunikimit publik dhe/ose sherbimeve te tyre nga aksesi i paautorizuar.

6. Operatoret duhet te menaxhojne dhe mbrojne pajisjet dhe sistemet e perdorura per ruajtjen e te dhenave te perdoruesve te rrjeteve te komunikimit publik dhe/ose sherbimeve te tyre nga aksesi, humbja, modifikimi aksidental dhe/ose i paautorizuar.

7. Operatoret duhet të sigurojnë një nivel të mbrojtjes dhe sigurisë së përshtatshme ndaj rreziqeve të mundshme, të parashikuara. Masat qe operatoret do te ndermarrin duhet që, të paktën:

   a) të sigurojnë që të dhënat personale të jenë të aksesueshme vetëm nga personeli i autorizuar për qëllime ligjore të autorizuara;

   b) të mbrojnë të dhënat personale të ruajtura ose të transmetuara nga aksidentet apo nga shkatërrimi i kundërligjshëm, humbja ose ndryshimi aksidental dhe ruajtja, përpunimi, aksesi apo zbulimi i paautorizuar ose i jashtëligjshëm;

   c) të sigurojnë implementimin e politikave të sigurisë, lidhur me përpunimin e të dhënave personale.

8. Operatoret duhen te kene rregullore ne lidhje me sigurine ose rregulla te mirepercaktuara, te publikuara dhe rregullisht te perditesuara per menaxhimin e rrjeteve dhe sherbimeve te komunikimeve elektronike publike.

9. Operatoret duhet te percaktojne minimalisht nje person te autorizuar qe do te jete pergjegjes per monitorimin e zbatimit te ketyre detyrimeve ne lidhje me sigurine si dhe është personi i kontaktit për komunikimin me AKEP ne rast të ndodhjes se nje incidenti sigurie.

10. Operatoret detyrimisht duhet te kene planin e vazhdimesise se ofrimit te rrjeteve te komunikimit publik dhe/ose sherbimeve te komunikimeve publike, I cili do të applikohet menjëherë ne momentin kur ndodh nje incident sigurie.

11. Operatoret duhet te publikojne ne ëebsite-t e tyre manuale per perdoruesit rreth incidenteve me te zakonshme te sigurise, veprimeve dhe/ose mjeteve qe duhen ndjekur per te parandaluar ndodhjen e ketyre incidenteve dhe veprimeve qe duhen ndjekur pas ndodhjes se incidenteve te sigurise.

12. Operatoret duhet te informojne perdoruesit e sherbimeve te rrjeteve te komunikimit publik ne lidhje me punet e planifikuara per mirembajtjen ose perditesimet, të paktën 1 dite përpara fillimit të punimeve te cilat mund te sjellin nderprerje provizore te sherbimeve.

13. Operatoret janë të detyruar të informojnë përdoruesit e tyre për një rrezik të veçantë, mënyrën se si rreziku mund të reduktohet nga përdoruesit, si dhe kostot e mundshme, që duhet të mbulohen nga përdoruesi, nëse rreziku që ndodh është jashtë masave, që mund të marrë sipërmarrësi.

14. Në rast të cenimit të të dhënave personale, sipërmarrësi që ofron shërbime të komunikimeve elektronike të vlefshme për publikun njofton pa vonesë AKEP-in për këtë shkelje.

15. Kur një shkelje e të dhënave personale mund të ndikojë në privatësinë e pajtimtarit ose individit, sipërmarrësi, gjithashtu, njofton pa vonesë pajtimtarin ose individin për shkeljen.

16. Pa paragjykim ndaj detyrimit të sipërmarrësit për të njoftuar pajtimtarët dhe individët në fjalë, nëse sipërmarrësi nuk e ka njoftuar pajtimtarin ose individin për shkelje të të dhënave personale, AKEP-i, pasi të ketë marrë parasysh ndikimin e shkeljes, mund të kërkojë që sipërmarrësi të njoftojë pajtimtarin.

17. Njoftimi I pajtimtarit/ individit , përshkruan të pakten natyrën e shkeljes së të dhënave personale dhe personin e kontaktit ku mund të merret informacion më i detajuar, si dhe rekomandon masa për të minimizuar efektet e mundshme të këqija të shkeljes së të dhënave personale.

18. Sipërmarrësit mbajnë një regjister/ evidenca të plota të shkeljeve të të dhënave personale, që përmban fakte lidhur me këto shkelje, ndikimin e tyre dhe masat e ndërmarra.

19. Operatoret qe kryejne transaksione financiare online, duhet ti ushtrojnë ato ne perputhje me standartin PCI DSS (Payment Card Industry Data Security Standard).

Neni 7

Detyrimet e AKEP

1. Garanton ruajtjen e integritetit te te dhenave te operatoreve te rrjeteve dhe/ose sherbimeve te komunikimeve elektronike publike nga modifikimet e tyre jo te autorizuara ose jo te kerkuara nga operatori perkates.
2. Garanton ruajtjen e konfidencialitetit te te dhenave te operatoreve te rrjeteve dhe/ose sherbimeve te komunikimeve elektronike publike prej personave jo te autorizuar me perjashtim te kerkesave që vinë nga organe dhe institucione sipas legjislacionit në fuqi.

3. ushtron kompetencat
4.
5. ne perputhje me Ligjin e Mbrojtjes se te Dhenave Personale dhe aktet nënligjore në zbatim të tij.
6. Investigon Nese e shikon te nevojshme, mbi incidentet e sigurise te raportuara nga operatoret duke ruajtur gjithmone sekretin dhe anonimatin e hetimit.
7. Njofton perdoruesit e rrjeteve dhe/ose sherbimeve rreth incidentit te sigurise, në rast se e konsideron si te larte impaktin e incidentit te sigurise,
8. Kryen kontrolle ne menyre periodike ne bashkepunim me ALCIRT, per te verifikuar implemetimin e kesaj rregulloreje.
9. Ndermerr masa sipas legjislacionit në fuqi nese operatoret nuk plotesojne kërkesat dhe kushtet e kesaj rregulloreje.

Neni 8

Konfidencialiteti i Komunikimeve

1. Konfidencialiteti i komunikimeve dhe i trafikut te te dhenave ne rrjetet e komunikimeve elektronike publike dhe/ ose ne sherbimet e tyre duhet te garantohet nga ofruesit e tyre. Operatoret ne menyre specifike duhet te parandalojne pergjimin ose interceptimin e thirrjeve telefonike ose format e tjera te pergjimit te komunikimeve dhe trafikut te te dhenave nga persona pertej atyre te perfshire direkt ne komunikim, me perjashtim te rastit kur dicka e tille eshte ligjerisht e autorizuar.

2. Përjashtohen nga detyrimi i përcaktuar në Pikën 1 regjistrimet e autorizuara ligjerisht te komunikimeve kur ndermerren ne kuadrin e praktikave te ligjeruara te biznesit per qellimin e ofrimit te evidences te nje transaksioni komercial ose te ndonje komunikimi tjeter biznesi.

3. Operatoret duhet te garantojne perdorimin e mjeteve te duhura ne sistemet e komunikimeve elektronike dhe ne sistemet e procesimit te te dhenave per te mbajtur sekret komunikimet elektronike dhe te dhenat personale te perdoruesve, po keshtu per te ndaluar aksesin e paautorizuar ne keto sisteme.

4. Operatoret, personat e autorizuar, punonjesit, dhe cdo individ i përfshirë në sistemet e komunikimeve elektronike, pjesë e strukturave të Operatorit jane pergjegjes per ruajtjen dhe mbrojtjen e konfidencialitetit te te dhenave dhe komunikimeve.

5. Operatoret duhet te mbledhin te dhena ne lidhje me perdoruesit e tyre vetem për qëllim dhe deri ne shkallen e nevojshme per te kryer detyren e tyre te ofrimit te sherbimeve te komunikimeve publike.

6. Operatoret duhet te informohen ne lidhje me mesazhet ose te dhenat e transmetuara permes rrjetit te tyre vetem deri ne shkallen e nevojshme per te kryer detyren e tyre te ofrimit te sherbimeve te komunikimeve publike.

7. Marrja, regjistrimi, publikimi dhe perdorimi i te dhenave dhe mesazheve te transmetuar nga rrjetet e komunikimit publik dhe qe nuk jane te destinuara per publikun, po keshtu dhe shperndarja e tyre te njerez te paautorizuar jane te ndaluara nese nuk parashikohet ndryshe nga legjislacioni ne fuqi.

Neni 9

Vleresimi i Impaktitte Incidenteve te Sigurise

1. Operatoret duhet te kryjne vleresimin e impaktit te incidenteve te sigurise sipas tabeles se paraqitur ne Aneksin 2.

2. Incidentet e sigurise qe kane pasur kohezgjatje me pak se 1 ore, ne menyre automatike konsiderohen si te nje impakti te ulet dhe nuk eshte i nevojshem plotesimi i tabeles.

3. Incidentet e sigurise konsiderohen si incidente me impakt te larte nese numri i perdoruesve te ndikuar nga incidenti ose perqindja e tyre (%) ndaj perdoruesve total eshte minimalisht 1000 ose 5%.

4. Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtrirjes se tij eshte minimalisht 10 km².

5. Ne cdo rast tjeter, incidentet e sigurise konsiderohen si incidente me impakt mesatar.

6. Ne vleresimin perfundimtar te impaktit, duhet patur parasysh se nese incidenti i sigurise eshte konsideruar i larte nga minimalisht 1 parameter (mesatar nga parametri tjeter), atehere ai konsiderohet nje incident me impakt te larte dhe ne vleresimin perfundimtar.

7. Tabela per vleresimin e impaktit te incidentit te sigurise mund te riplotesohet sa here qe kemi nje ndryshim te parametrave ne lidhje me kohezgjatjen e incidentit te sigurise, numrin e perdoruesve te prekur dhe zonen gjeografike te shtrirjes se incidentit te sigurise.

8. Brenda 15 diteve pune pas perfundimit te incidentit te sigurise, operatoret duhet te kryejne vleresimin perfundimtar te impaktit te incidentit te sigurise.

Neni 10

Raportimi i masave te sigurise dhe auditit

1. Sipermarresit e shërbimeve te komunikimeve elektronike qe rezultojne sipas raportimeve te kryera ne AKEP me të ardhura vjetore te vitit paraardhes nga komunikimet elektronike nen vleren 100,000,000 leke duhet te raportojne ne AKEP ne formen e nje vetedeklarimi periodikisht nje here ne vit brenda muajit Janar per vitin paraardhes sipas Aneks 3.

2. Sipermarresit e komunikimeve elektronike qe rezultojne sipas raportimeve te kryera ne AKEP me të ardhura vjetore te vitit paraardhes nga komunikimet elektronike mbi vleren 100,000,000 leke , duhet qe te dorezojne prane AKEP raportin me rezultatet e auditit të sigurisë, të kryer nga një organ i certifikuar dhe i pavarur ose nga autoriteti kompetent. Raporti duhet te dorezohet periodikisht per nje periudhe jo me shume se dy vjecare. Kostoja e auditit do të paguhet nga sipërmarrësi.

Neni 11

Raportimi i Incidenteve te Sigurise

AKEP-i kërkon që sipërmarrësit të ofrojnë informacion të nevojshëm për të vlerësuar sigurinë dhe/ose integritetin e shërbimeve dhe rrjeteve, duke përfshirë politika të dokumentuara të sigurisë

1

2. Operatoret duhet te njoftojne dhe te dergojne formularin e aneksit 1 prane Autoritetit jo me vone se brenda 3 diteve nga momenti i zbulimit te incidentit te sigurise. Kjo duhet bere vetem pas vleresimit te impaktit te sigurise dhe vetem nese ai rezulton mesatar ose i larte.

3. Ky njoftim i pare duhet te permbaj te pakten informacionet e meposhtme:

a) vleresimin se cilat rrjete ose sherbime te komunikimit publik jane ndikuar ose do te ndikohen nga incidenti i sigurise,

b) vleresimin e zones gjeografike qe eshte dhe/ose do te ndikohet nga incidenti i sigurise,

c) vleresimin e segmentit te perdoruesve qe jane ndikuar ose do te ndikohen nga incidenti i sigurise,

d) vleresimin e planit te rimekembjes,

e) vleresimin paraprak te shkakut ose shkaqeve, qe operatori mendon se kane shkaktuar incidentin e sigurise.

4 .Njoftimi fillestar dergohet te AKEP permes e-mailit incidente.raportimi@akep.al dhe /ose permes insrumentave te tjere te vene ne dispozicion per kete qellim nga AKEP.

5. Ne rastin ku kemi nje ndryshim te rendesishem te te dhenave te percaktuara ne piken 4, operatori paraqet shpejt prane AKEP nje njoftim te ri.

6. Brenda 15 diteve nga ndodhja e incidentit te sigurise, operatoret duhet te paraqesin njoftimin perfundimtar ne lidhje me incidentin e sigurise. Njoftimi perfundimtar dergohet ne AKEP sipas percaktimeve te pikes 4.

7. AKEP mund te kerkoj te dhena te tjera shtese, pervec atyre ne formularin perfundimtar, ne lidhje me incidentin e sigurise. Per kete arsye, operatoret jane te detyruar te ruajne te gjithe te dhenat ne lidhje me incidentet e sigurise se raportuar per nje periudhe kohore prej 18 muaj qe nga koha e dorezimit te njoftimit perfundimtar rreth incidentit te sigurise.

Neni 11

Investigimi i Incidenteve te Sigurise dhe Cenimit te Integritetit

Duke vleresuar nivelin e riskut te incidentit te sigurise dhe/ ose cenimit te integritetit te raportuar sipas Formularit ne aneksin 1, AKEP mund te ndermarre veprimet e nevojshme per investigimin e ketij incidenti te sigurise dhe po ashtu per sqarimin e te gjitha rrethanave percaktuar nga njoftimi i operatorit.

Nese eshte e nevojshme, ne kuader te investigimit, AKEP do te informoj Agjensine Kombetare te Sigurise Kompjuterike (ALCIRT) dhe organet e tjera konpetente ne perputhje me legjislacionin për transmetimin e te dhenave nderkombetare.

Per arsye sigurie, AKEP mund te njoftoje publikun rreth incidenteve te sigurise, qe kane ndodhur ose qe mund te ndodhin ne te ardhmen ne komunikimet elektronike publike edhepa marre pelqimin paraprak te operatorit.

Neni 12

Zbatimi i rregullores

1. Te gjithe sipermarresit e komunikimeve elektronike publike janë të detyruar të zbatojnë kete rregullore.Sipermarresit do te jene subjekt i masave administrative nese ne kundershtim me kete rregullore:

- nuk kane permbushur nje ose disa nga detyrimet e nenit 3.
- nuk kane raportuar prane AKEP incidente te sigurise te nje impakti mesatar dhe/ose te larte.

- nuk kane respektuar afatet e njoftimit dhe raportimit prane AKEP te incidenteve te sigurise.
- kane bere nje vleresim jo te vertete te impaktit te incidentit te sigurise duke menjanuar ne kete menyre detyrimin e raportimit.
- kane plotesuar formularin ne Aneks 1 me te dhena te rreme ose nuk e kane plotesuar ne menyre te plote.
- nuk kane ruajtur te dhenat ne lidhje me incidentet e sigurise se raportuar per nje periudhe kohore prej 18 muaj qe nga koha e dorezimit te njoftimit perfundimtar rreth incidentit te sigurise.

2. Moszbatimi i detyrimeve qe rrjedhin nga kjo rregullore përbën kundravajtje administrative dhe ne keto raste do te zbatohet neni 137 i ligjit Nr.9918 datë 19.05.2008 "Për komunikimet elektoronike në Republikën e Shqipërisë", i ndryshuar.

Neni13

Informimi dhe publikimi

Kjo rregullore eshte pjesë e akteve rregullatore të nxjerra nga AKEP dhe publikohet në faqen e internetit të AKEP-it me hyrjen ne fuqi te saj.

Neni 14
Hyrja në fuqi dhe vlefshmëria

Kjo rregullore dhe Anekset e saj hyjne në fuqi pas miratimit me vendim të Këshillit Drejtues.
Cdo document apo dispozitë tjeter që bie ne kundershtim me kete Rregullore shfuqizohet.

ANEKS 1

FORMULARI PER RAPORTIMIN E NJE INCIDENTI TE SIGURISE DHE/OSE CENIMIT TE INTEGRITETIT	
Informacion Kontakti	*Emri i Operatorit:*
	Emri dhe Mbiemri i personit te ngarkuar me eleminimin e incidenteve te sigurise dhe/ose cenimit te integritetit:
	Pozicioni i Punes:
	Adresa:
	Telefon, e-mail:
Pershkrimi i Incidentit te Sigurise dhe/ose Cenimit te Integritetit	*Lloji:*
	Percaktimi se cila rrjete, sisteme ose sherbime preken na incidenti i sigurise:
	Koha e ndodhjes dhe kohezgjatja:

	Informacion rreth shkakut fillestar ose shkaqeve:
	Pershkrimin e incidentit (percaktoni te dhenat ne menyre sa me te detajuar):
	Numri i perafert i perdoruesve te prekur nga incidenti i sigurise ose cenimi i integritetit ose perqindja e tyre(%) nga perdoruesve total te rrjetit dhe/ose sherbimit:
	Zona Gjeografike e prekur nga incidenti i sigurise dhe/ose cenimi i integritetit:

	Burimet e prekura
	Pasojat :
Menaxhimi i incidentit te sigurise dhe/ose cenimit te integritetit	*Veprimet e ndermarra(te planifikuara per tu ndermarre) per te eleminuar incidentin e sigurise dhe per te reduktuar pasojat e tij:* *Masat pas incidentit*
Informacione te Tjera te Rendesishme	*Mesimet e nxjerra*
Data	
Formulari depozitohet pranë Autoritetit Përgjegjës me:Fax:+355 4 2259 106 ose E-mail (te skanuara) ne adresen: incidente.raportimi@akep.al	

Fushat e Formularit të Raportimit të Incidenteve

Në këtë pjesë, do të përshkruhen fushat e raportimit të incidenteve, që duhet të përdoren nga Autoritetet Rregullatore kur dërgojnë raporte të incidenteve te ENISA dhe Komisioni Europian, si pjesë e raportimit përmbledhës vjetor.

Shërbimet e prekura

Në fushën "shërbimi i prekur", Autoritetet Rregullatore duhet të japin informacion se cila shërbime të komunikimeve elektronike janë prekur, për shembull duke përcaktuar një ose disa nga:

- Telefonia fikse
- Telefonia e lëvizshme
- Akses i internetit nëpërmjet rrjetit fiks
- Akses i internetit nëpërmjet rrjetit mobile

Ose në mënyrë alternative, autoritetet rregullatore mund të përcaktojnë se një lloj tjetër shërbimi është prekur. Po kështu, në mënyrë opsionale, autoritetet mund të japin informacione të mëtejshme rreth teknologjisë ose platformës së prekur.

Për shembull, nëse një stuhi rrëzon një numër të stacioneve bazë mobile, duke shkaktuar dëmtim të rrjetit, shërbimi i prekur në këtë incident do të jetë telefonia e lëvizshme, interneti nëpërmjet rrjetit mobile dhe vecanërisht GSM, GPRS/EDGE, UMTS, për të shpjeguar llojin e teknologjisë ose platformës së prekur.

Numri i përdoruesve

Në fushën "Numrin i përdoruesve", autoritetet rregullatore duhet të përcaktojnë numrin total të përdoruesve të prekur.

- Për telefoninë fikse dhe aksesin në internet nëpërmjet rrjetit fiks, autoritetet rregullatore duhet të raportojnë numrin e pajtimtarëve ose linjat e aksesit të prekura.
- Për telefoninë e lëvizshme dhe aksesin në internet nëpërmjet këtij rrjeti, autoritetet rregullatore duhet të raportojnë një vlerësim ose parashikim, duke marrë në konsideratë përdorimin normal të burimeve të prekura.

Për shembull, nëse një stacion bazë, i cili i shërben 1000 përdoruesve në orë mesatarisht, është jashtë shërbimit për një orë, atëherë impakti i këtij incidenti duhet vlerësuar si 1000 përdorues.

Duhet patur parasysh që në shumë incidente, disa shërbime janë të prekura në të njëjtën kohë dhe si pasojë numri i përdoruesve të prekur do të jetë i ndryshëm për cdo shërbim. Në këto raste, autoritetet rregullatore duhet të paraqesin të dhëna për cdo shërbim.

Duhet patur parasysh gjithashtu se ofruesit e shërbimeve, jo gjithmonë, kanë një përcaktim ekzakt të numrit të përdoruesve të prekur, sepse ata shpërndajnë shërbime në ofrues të tjerë (quhen shpesh rishitës, ose përdorues të ndërmjetëm). Ofruesi, në këtë rast, jo gjithmonë di numrin e saktë të përdoruesve (ose klientëve sic referohen në Direktivë) të fundit dhe rrjedhimisht nuk mund të njoh numrin e saktë të përdoruesve të prekur nga një incident. Në këto raste, autoritetet rregullatore duhet të raportojnë vlerësime ose parashikime.

Kohëzgjatja

Në fushën "kohëzgjatja", autoritetet rregullatore duhet të përcaktojnë afatin e kohës (në orë), gjatë të cilave ka patur impakt të rëndësishëm në funksionimin e shërbimeve.

Për shembull, supozojmë se një stuhi shkakton ndërprerje të energjisë elektrike nga mesnata deri në orën 6 të mëngjesit dhe supozojmë që shërbimi i telefonisë celulare preket nga ora 4 (kur energjia backup harxhohet) deri në 7 të mëngjesit. Në këtë rast, kohëzgjatja e incidentit është 3 orë.

Impakti në thirrjet e emergjences

Në fushën "impakti në thirrjet emergjente", autoritetet rregullatore duhet të përcaktojnë nëse ka patur një impakt në mundësinë për të telefonuar shërbimet e emergjencës, si ambulancën ose zjarrfikëset nëpërmjet numrave të emergjencës (112 në shumë vende).

Për shembull, supozojmë se qendra operative e një operatori telefonik ka një ndërprerje energjie, që pengon shumë zona të një vendi të lidhen me 112. Në këtë rast, incidenti ka një impakt në thirrjet e emergjencës.

Impakti në Interkoneksion

Në fushën "Impakti në Interkonjeksionet", autoritetet rregullatore duhet të përcaktojnë nëse ka ndonjë impakt në interkonjeksionet kombëtare dhe ndërkombëtare midis ofruesve.

Për shembull, supozojmë se një pikë e madhe shkëmbimi internet preket nga një ndërprerje e energjisë duke shkaktuar problem të mëdha të shërbimit internet. Në këtë rast, incidenti ka një impakt në interkonjeksionet.

Kategoria e shkakut fillestar

Shkaku kryesor i një incidenti është shkaku fillestar i incidentit, ose me fjalë të tjera, eventi ose faktori që nxiti incidentin. Në fushën "kategoria e shkakut fillestar", autoritetet rregullatore duhet të përcaktojnë kategorinë e shkakut fillestar, nxitës së incidentit. Kemi 5 kategori të shkakut fillestar:

Gabimet Njerëzore

Kategoria “gabimet njerëzore” duhet të përdoret për incidentet e shkaktuara nga gabimet njerëzore gjatë funksionimit të pajisjeve ose burimeve, përdorimin e mjeteve, ekzekutimin e procedurave etj.

Për shembull, supozojmë se një punonjës i një ofruesi kryen një gabim në procedurat e mirëmbajtjes së një pajisjeje duke shkaktuar mosfunksionimin e saj.Në këtë rast, incidenti duhet të jetë në kategorinë burimet njerezore si shkak fillestar ose nxitës i incidentit.

Dështimet e Sistemit

Kategoria ‘Dështimet e Sistemit”, duhet të përdoret për incidentet e shkaktuara nga dështimet e sistemit për shembull dështimet hardëare, softëare ose shkeljet e manualeve, procedurave ose politikave.

Për shembull, supozojmë se një ofrues ka një program të plotë mirëmbajtjeje për pajisjet e saj, dhe gjeneratorët diesel nuk janë të përfshirë në këtë program. Si pasojë, gjeneratori dështon për arsye se nuk ka një program mirëmbajtjeje për të. Në këtë rast, shkaku fillestar, nxitës i incidentit duhet të jetë në kategorinë e Dështimeve të Sistemit.

Dukuritë Natyrore

Kategoria “Dukuri Natyrore” duhet të përdoret për incidente që shkaktohen nga moti i përkeqësuar, tërmetet, përmbytjet, pandemitë, zjarret ose kafshët e egra etj.

Për shembull, supozojmë se ketrat presin kabllot, duke shkaktuar ndërprerje, atëherë incidenti duhet të jetë në kategorinë e shkakut fillestar si Dukuri Natyrore.

Veprimet e dëmshme

Kategoria “veprimet e dëmshme”duhet të përdoret për incidentet e shkaktuara nga veprimi i paramenduar i një personi ose i një grupi.

Për shembull, incidentet që kanë si arsye fillestare zjarrvënien nga punonjësit si një akt sabotazhi, ndërhyrja në sistemet DNS nga kriminelët, hackimi i sistemeve kompjuterike të ofruesit e kështu me rradhë.

Dështimet e palëve të treta

Kategoria “dështime nga palë të treta”, duhet të përdoret për incidente ku shkaku fillestar ose nxitës është jashtë kontrollit direkt të ofruesit, për shembull, kur shkaku fillestar ndodh te një kontraktor që përdoret për outsourcing ose te një organizatë furnitore.

Kjo kategori mund të përdoret më vete kur shkaku fillestar ose nxitës i incidentit është i panjohur. Në rastet e tjera, kjo kategori duhet të përdoret së bashku me një nga kategoritë e tjera të shkakut fillestar ose iniciues.

Për shembull, një ndërprerje e shkaktuar nga prerja e kabujve nga një makinë gërmimi gjatë ndërtimit të një rruge të re, mund të kategorizohet në kategorinë gabime njerëzore dhe dështime të palëve të treta.

Shkaku Fillestar

Në fushën "Shkaku Fillestar", autoritetet rregullatore duhet të përcaktojnë shkakun fillestar të incidentit, për shembull eventin ose faktorin që nxit incidentin.

Për shembull, shkaqet fillestare mund të jenë dështimet softëare, ndërprerjet e energjisë elektrike, sulmet kibernetike, harxhimi i karburantit backup e kështu me rradhë.

Duhet patur parasysh që këto shkaqe të detajuara mund të kategorizohen në kategori të ndryshme të shkakut nxitës, në varësi të specifikave të tij. Për shembull, një prerje kablli mund të shkaktohet nga një gabim njerëzor ose nga një defekt në procedurë.

Shkaqet e Tjera

Shpesh incidentet përfshijnë një sërë eventesh ose faktorësh. Në fushën "shkaku tjetër", autoritetet rregullatore mund të përcaktojnë një shkak (shih në listën e shkaqeve në sektorin 7.1.7), që ka luajtur një rol në incident.

Për shembull, një stuhi shkakton një ndërprerje të kabujve që sjell një ndërprerje të energjisë, kështu që në këtë rast shkaku fillestar është stuhia dhe shkaku tjetër ose pasues është ndërprerja e kabujve.

Burimet e Prekura

Autoritetet rregullatore duhet të përcaktojnë burimet ose asetet e prekura nga incidenti.

Për shembull, asetet e prekura mund të jenë stacionet bazë mobile, kabinat e rrugës, sëitchet, backbone ndërkombëtar e kështu me rradhë.

Përshkrimi i Incidentit

Në fushën "Përshkrimi i Incidentit", autoritetet rregullatore duhet të ofrojnë një përshkrim të incidentit dhe sesi u zhvillua në fillim.

Veprimet e përgjigjes ndaj incidentit

Në fushën "Veprimet e përgjigjes ndaj incidentit", autoriteti duhet të jap një përshkrim të veprimeve të ndërmarra nga ofruesi për të reduktuar impaktin e incidentit.

Masat pas incidentit

Në fushën "Masat pas incidentit", autoriteti duhet të ofroj një përshkrim të veprimeve ose masave të ndërmarra nga ofruesi për të reduktuar probabilitetin e ndodhjes ose impaktin e incidenteve të ngjashme në të ardhmen.

Mësimet e nxjerra

Në fushën " Përshkrimi i mësimeve të nxjerra", autoriteti duhet të vendos një përshkrim të mësimeve të nxjerra nga incidentet ose masave afatgjate që do të implementohen nga autoriteti ose ofruesit.

ANEKS 2

TABELA PER VLERESIMIN E IMPAKTIT TE INCIDENTIT TE SIGURISE		
Kohezgjatja e incidentit te sigurise(nderprerjes se sherbimit, interceptimit te komunikimeve, softëare te demshem, vjedhja, modifikimi i te dhenave)	*Me teper se 1 ore, por me pak se 2 ore*	*Me teper se 2 ore*
Numri i perdoruesve te prekur nga incidenti ose % e tyre ndaj numrit total te perdoruesve te ofruesit		
>1000 ose >5%	*Mesatar*	*I Larte*
Ne rast te nje numri te panjohur te perdoruesve te prekur nga incidenti i sigurise, zona gjeografike e shtrirjes se incidentit te sigurise		
>10 km²	*Mesatar*	*I Larte*
Vleresimi Perfundimtar i Impaktit:	***Mesatar***	***I Larte***

ANEKS 3

Objektivat e Sigurisë dhe mjetet

Më poshtë listohen 25 objektivat e nivelit të lartë të sigurisë (SO1, SO2,…), të grupuara në 7 fusha (D1,D2,…). Për cdo objektiv të sigurisë, listohen masat e sigurisë që duhet të implementohen nga ofruesi i shërbimit për të plotësuar objektivin, po ashtu dhe faktet që duhen të merren në konsideratë nga një supervisor ose auditues kur vlerëson nëse mjetet apo masat mbrojtëse janë në funksion.

Më poshtë jepet një tabelë e përmbajtjes:

D1: Qeverisja dhe Menaxhimi i Riskut

SO 1: Politika e Sigurisë së Informacionit

SO 2: Qeverisja dhe Menaxhimi i Riskut

SO 3: Rolet e sigurisë dhe përgjegjësitë

SO 4: Siguria e aseteve të palës së tretë

D2: Siguria e Burimeve Njerëzore

SO 5: Kontrollet e Background-it

SO 6: Njohuria mbi sigurinë dhe trajnimi

SO 7: Ndryshimet e Personelit

SO 8: Trajtimi i Shkeljeve

D3: Siguria e sistemeve dhe pajisjeve

SO 9: Siguria Fizike dhe e Mjedisit

SO 10: Siguria e Burimeve

SO 11: Kontrolli i Aksesit në Rrjet dhe Sistemet e Informacionit

SO 12: Integriteti i Rrjetit dhe Sistemeve të Informacionit

D4: Menaxhimi i Operacioneve

SO 13: Procedurat Operacionale

SO 14: Menaxhimi I Ndryshimit

SO 15: Menaxhimi I Aseteve

D5: Menaxhimi I Incidenteve

SO 16: Procedurat e Menaxhimit të Incidenteve

SO 17: Aftësia e Zbulimit të Incidenteve

SO 18: Raportimi I Incidenteve dhe Komunikimi

D6: Menaxhimi I Vazhdimit të Biznesit

SO 19: Strategjia e Vazhdimit të Shërbimit dhe Planet e Emergjencës

SO 20: Aftësia e Rregullimit të Pasojave

D7 : Monitorimi, Auditimi dhe Testimi

SO 21: Politikat e Logimit dhe Monitorimit

SO 22: Planet e Emergjencave

SO 23: Testimi I Rrjetit dhe Sistemeve të Informacionit

SO 24: Vlerësimet e Sigurisë

SO 25: Monitorimi I Pajtueshmërisë

D1: Qeverisja dhe Menaxhimi i Riskut

Fusha "Qeverisja dhe Menaxhimi i Riskut mbulon objektivat e sigurisë që lidhen me qeverisjen dhe menaxhimin e risqeve të sigurisë së rrjetit dhe informacionit.

SO 1: Politika e Sigurisë së Informacionit

Vendos dhe mbaj një politikë të duhur të sigurisë së informacionit.

	Masat e Sigurisë	Evidenca
1	a) Vendos një politikë sigurie të nivelit të lartë që adreson sigurinë dhe vazhdimësinë e rrjeteve të komunikimit dhe/ose shërbimeve të ofruara prej tyre.	• Politikë sigurie e dokumentuar, duke përfshirë rrjetet dhe shërbimet, burimet kritike mbështetëse të tyre dhe objektivat e sigurisë. • Personeli kyc është në dijeni të politikës së sigurisë dhe objektivave

	b) Vëje ne dijeni personelin kyc për politikën e sigurisë.	të tij (intervista).
2	c) Vendos politika të detajuara të sigurisë së informacionit për asetet kritike dhe proceset e biznesit. d) Vendos në dijeni gjithë personelin për politikën e sigurisë dhe për cfarë lidhet me punën e tyre. e) Rishiko politikën e sigurisë pas incidenteve.	• Politika të sigurisë së informacionit të dokumentuara të aprovuara nga menaxhimi, duke përfshirë ligjin dhe rregulloret e zbatueshme, të arrishme nga personeli. • Personeli është në dijeni të politikës së sigurisë së informacionit dhe për cfarë lidhet me punën e tyre (intervista) • Rishiko komentet ose ndrysho pjesë të politikës.
3	f) Rishiko politikat e sigurisë së informacionit në mënyrë periodike dhe merr në konsideratë shkeljet, përjashtimet, incidentet e mëparshme, testet/ushtrimet e mëparshme dhe incidentet që kanë prekur ofruesit e tjerë në sektor.	• Politikat e sigurisë së informacionit janë të përditësuara dhe të miratuara nga menaxhimi i lartë. • Mbajtje e përjashtimeve të politikës, të miratuara nga rolet e përshtatshme. • Dokumentimi i procesit të rishikimit, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.

SO 2: Qeverisja dhe Menaxhimi i Riskut

Vendos dhe mirëmbaj një strukturë të duhur të qeverisjes dhe menaxhimit të riskut për të identifikuar dhe adresuar risqet për rrjetet dhe shërbimet e komunikimeve.

	Masat e Sigurisë	Evidenca
1	a) Bëj një listë të risqeve kryesore për sigurinë dhe vazhdimësinë e rrjeteve dhe/ose shërbimeve të ofruara të komunikimit, duke marrë në konsideratë kërcënimet kryesore për burimet e rëndësishme. b) Vendos në dijeni personelin kyc për risqet kryesore dhe sesi ti trajtosh ato.	• Listë e risqeve kryesore të përshkruara në një nivel të lartë, duke përfshirë rreziqet themelore dhe impaktin e tyre potencial në sigurinë dhe vazhdimësinë e rrjeteve dhe shërbimeve. • Personeli kyc duhet të dijë risqet kryesore (intervista).
2	c) Krijo dhe vendos një metodologji të menaxhimit të riskut dhe/ose mjetet bazuar në	• Metodologji dhe/ose mjetet e menaxhimit të riskut të dokumentuara.

	standartet e industrisë. d) Siguro që personeli kryesor përdor metodologjinë dhe mjetet e menaxhimit të riskut e) Rishiko vlerësimet e riskut pas ndryshimeve ose incidenteve. f) Siguro që risqet e mbetura pranohen nga menaxhimi.	• Udhëzimi për personelin në vlerësimin e risqeve. • Listë e risqeve dhe evidencë e rishikimeve/përditësimeve. • Rishiko komentet ose ndryshimet në vlerësimet e risqeve. • Miratimi i menaxhimit për risqet e mbetura.
3	g) Rishiko metodologjinë dhe/ose mjetet e menaxhimit të riskut, në mënyrë periodike, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	• Dokumentim i procesit të rishikimit dhe përditësimeve të metodologjisë dhe/ose mjeteve të menaxhimit të riskut.

SO 3: Rolet e Sigurisë dhe Përgjegjësitë

Vendos dhe mirëmbaj një strukturë të duhur të roleve të sigurisë dhe përgjegjësive.

	Masat e Sigurisë	Evidenca
1	a) Caktoji personelit rolet e sigurisë dhe përgjegjësitë . b) Siguro që rolet e sigurisë janë të arritshme në rast se ndodhin incidente sigurie.	• Listë e roleve të sigurisë (CISO, DPO, menaxher i vazhdimësisë së biznesit, etj) të cilët dhe informacione kontakti.
2	c) Personeli emërohet zyrtarisht në rolet e sigurisë. d) Vendos personelin në dijeni të roleve të sigurisë në organizatë dhe kur duhet të kontaktohen.	• Listë e emërimeve (CISO, DPO,etj) dhe përshkrimi i përgjegjësive dhe detyrave për rolet e sigurisë(CISO, DPO, etj) • Materiale ndërgjegjësimi dhe informimi për personelin duke shpjeguar rolet e sigurisë dhe kur/si ata duhet të kontaktohen.
3	e) Struktura e roleve të sigurisë dhe përgjegjësive rishikohet rregullisht, si pasojë e ndryshimeve dhe/ose incidenteve të mëparshme.	• Dokumentim i përditësuar i strukturës së detyrave të roleve të sigurisë dhe përgjegjësive. • Dokumentim i procesit të rishikimit, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.

SO 4: Siguria e aseteve të palës së tretë

Vendos dhe mirëmbaj një politikë me kërkesa sigurie për kontratat me palët e treta për të garantuar që varësitë me palët e treta nuk ndikojnë negativisht sigurinë e rrjeteve dhe/ose shërbimeve.

	Masat e Sigurisë	Evidenca
1	a) Përfshini kërkesat e sigurisë në kontratat me palët e treat.	• Kërkesa të qarta të sigurisë në kontratat me palët e treat që na furnizojnë me produkte IT, shërbime IT, procese biznesi outsource, helpdesks, call center, ndërlidhje, pajisje të përbashkëta, etj.
2	b) Vendos një politikë sigurie për kontratat me palët e treta. c) Siguro që të gjitha prokurimet e shërbimeve/produkteve nga palët e treta janë në përputhje me politikën. d) Rishiko politikën e sigurisë për palët e treta, pas incidenteve ose ndryshimeve. e) Redukto risqet e mbetura që nuk janë të adresuara nga pala e tretë.	• Politikë sigurie e dokumentuar për kontratat me palët e treta. • Listë e kontratave me palët e treta. • Kontratat për shërbime me palë të treta përmbajnë kërkesa sigurie në përputhje me politikën e sigurisë për prokurimet. • Rishiko komentet ose ndryshimet e politikës. • Risqet e mbetura që rezultojnë nga varësitë me palët e treta listohen dhe trajtohen.
3	f) Mbaj rekorde të incidenteve të sigurisë të lidhura ose të shkaktuara nga palët e treta. g) Rishikim dhe përditësim të politikës së sigurisë për palët e treta në intervale të rregullta, duke marrë në konsideratë incidentet dhe ndryshimet e mëparshme.	• Listë e incidenteve të sigurisë të lidhura ose të shkaktuara nga angazhimi me palët e treta. • Dokumentim i procesit te rishikimit të politikës.

D2: Siguria e Burimeve Njerëzore

Fusha Siguria e Burimeve Njerëzore mbulon objektivat e sigurisë që lidhen me personelin.

SO 5: Kontrollet e Background-it

Kryej kontrolle te duhura background mbi personelin (punonjësit, kontraktorët dhe përdoruesit e palëve të treta) nëse kërkohet për detyrimet dhe përgjegjësitë e tyre.

	Masat e Sigurisë	Evidenca
1	a) Kontrollo referencat profesionale të personelit kyc(	• Dokumentim i kontrollove të referencave profesionale për

	administratorit të sistemit, oficerëve të sigurisë, etj)	personelin kyc.
2	b) Kryej verifikime të background-it për personelin kyc, kur nevojitet dhe lejohet ligjerisht. c) Vendos një politikë dhe procedurë për kontrollet e background-it.	• Politikë dhe procedurë për kontrollet e background-it. • Udhëzim për personelin se kur/si të kryej kontrolle të background-it.
3	d) Rishiko dhe përditëso politikën/procedurat për kontrollet e background-it dhe referencës në mënyrë periodike, duke marrës në konsideratë ndryshimet dhe incidentet e mëparshme.	• Rishiko komentet ose ndryshimet e politikës/procedurës.

SO 6: Njohuria mbi sigurinë dhe trajnimi

Siguro që personeli ka njohuri të mjaftueshme mbi sigurinë dhe kryejnë trajnime të rregullta.

	Masat e Sigurisë	Evidenca
1	a) Garanto personelin kyc me trajnime dhe materiale të përshtatshme mbi cështjet e sigurisë.	• Personeli kyc ka ndjekur trajnime të sigurisë dhe ka njohuri të mjaftueshme mbi sigurinë (intervista).
2	b) Implemento një program për trajnimin, duke bërë të sigurt që personeli kyc ka njohuri të përditësuara dhe të mjaftueshme mbi sigurinë. c) Organizo trajnime dhe sesione ndërgjegjësimi për personelin në cështjet e sigurisë për organizatën.	• Personeli ka marrë pjesë në sesione ndërgjegjësimi në cështjet e sigurisë. • Program të dokumentuar për trajnimin mbi aftësitë e sigurisë, duke përfshirë objektivat për role të ndryshme dhe sesi të arrihen ato.
3	d) Rishiko dhe përditëso programin e trajnimit në mënyrë periodike, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme. e) Testo nivelin e njohurive mbi sigurinë të personelit.	• Program i përditësuar për ndërgjegjësimin dhe trajnimin mbi sigurinë. • Rezultatet e testeve mbi njohuritë e sigurisë të personelit. • Rishiko komentet ose ndryshimet për programin.

SO 7: Ndryshimet e Personelit

Vendos dhe mirëmbaj një process të duhur për menaxhimin e ndryshimeve në personel ose ndryshimet në rolet dhe përgjegjësitë e tyre.

	Masat e Sigurisë	Evidenca
1	a) Kur ka ndryshime në personel, hiq të drejtat e aksesit, badget, pajisjet, etj kur nuk nevojiten më. b) Eduko personelin e ri për politikat dhe procedurat.	• Evidencë që ndryshimet e personelit kanë pasuar me heqjen e të drejtave të aksesit, badget, pajisjet etj. • Evidencë që personeli i ri është edukuar rreth politikave dhe procëdurave.
2	c) Implemento politikë/procedura për ndryshimet e personelit, duke marrë në konsideratë heqjen në kohë të të drejtave të aksesit, badget, pajisjet. d) Implemento politikën/procedurat për edukimin dhe trajnimin për personelin në rolet e reja.	• Dokumentim të procesit të ndryshimeve të personelit, duke përfshirë përgjegjësitë për menaxhimin e ndryshimeve, përshkrimin e të drejtave të aksesit dhe posedimit të aseteve për cdo rol, procedurat për edukimin dhe trajnimin e personelit në rolet e reja. • Evidencë që ndryshimet e personelit janë kryer në bazë të procesit dhe që të drejtat e aksesit janë përditësuar në kohën e duhur.
3	e) Kontrolle periodike që politika/procedurat janë efektive. f) Rishiko dhe vlerëso politikën/procedurat për ndryshimet e personelit, duke marrë në konsideratë ndryshimet ose incidentet e mëparshme.	• Evidencë e kontrolleve mbi të drejtat e aksesit. • Politikë/procedura të përditësuara për menaxhimin e ndryshimeve në personel. • Rishiko komentet ose ndryshimet.

SO 8: Trajtimi i Shkeljeve

Vendos dhe mirëmbaj një process të disiplinuar për punonjësit që shkelin politikat e sigurisë ose një process më të gjerë që mbulon thyerjet e sigurisë të shkaktuara nga personeli.

	Masat e Sigurisë	Evidenca
1	a) Mbaj personelin të përgjegjëshëm për thyrjet e sigurisë të shkaktuara nga shkeljet e politikave, për shembull përmes kontratave të punës.	• Rregulla për personelin, duke përfshirë përgjegjësitë, kodin e sjelljes, thyerjet e politikave etj, mundësisht si pjesë e kontratave të punës.
2	b) Vendos procedura për shkeljet	• Dokumentim i procedurës, duke

	e politikave nga personeli.	përfshirë llojet e shkeljeve, që mund të jenë subjekt i masave disiplinore
3	c) Rishikim dhe përditësim periodik i procesit disiplinor duke u bazuar në ndryshimet dhe incidentet e mëparshme.	• Rishiko komentet ose ndryshimet.

D3: Siguria e Sistemeve dhe Pajisjeve

Kjo fushë "Siguria e Sistemeve dhe Pajisjeve"mbulon sigurinë fizike dhe logjike të rrjetit, sistemeve të informacionit dhe pajisjeve.

SO 9: Siguria Fizike dhe e Mjedisit

Vendos dhe mirëmbaj një siguri të duhur fizike dhe të mjedisit të rrjetit, sistemeve të informacionit dhe pajisjeve.

	Masat e Sigurisë	Evidenca
1	a) Elemino aksesin fizik të paautorizuar te pajisjet dhe infrastruktura dhe kryej kontrolle mjedisore për mbrojtjen ndaj hyrjes së paautorizuar, vjedhjes, zjarrit, përmbytjeve etj.	• Implementim bazë të masave të sigurisë fizike dhe kontrolleve mjedisore, si cëlsa, alarm ndaj vjedhjes, zjarrit, dhe sisitemin për shuarjen e tij etj.
2	b) Implemento një politikë të masave të sigurisë fizike dhe kontrolleve të mjedisit. c) Implementim i standarteve të industrisë mbi kontrollet fizike dhe të mjedisit.	• Politikë e dokumentuar për masat e sigurisë fizike dhe kontrolleve të mjedisit, duke përfshirë përshkrimin e pajisjeve dhe sistemeve. • Kontrolle fizike dhe të mjedisit, si kontrollin elektronik të hyrjes dhe mjete të gjurmimit, ndarje të hapësirave sipas niveleve të autorizimit, fikëse automatike zjarri etj.
3	d) Vlerëso efektivitetin e kontrolleve fizike dhe të mjeditit periodikisht. e) Rishiko dhe përditëso politikën për masat e sigurisë fizike dhe kontrollet e mjedisit duke marrë në konsideratë ndryshimet dhe incidentet e	• Politikë e përditësuar për masat e sigurisë fizike dhe kontrollet e mjedisit. • Dokumentim të vlerësimit të kontrollit mjedisor, rishiko komentet ose ndryshimet.

	mëparshme.	

SO 10: Siguria e Burimeve

Vendos dhe mirëmbaj një siguri të duhur të burimeve (elektricitet, karburant etj)

	Masat e Sigurisë	Evidenca
1	a) Garanto sigurinë e burimeve si energjia elektrike, karburanti ose ftohësi.	• Siguria e burimeve mbrohet në një mënyrë bazike, për shembull përmes linjave backup të energjisë elektrike ose burimeve alternative të karburantit.
2	b) Implemento një politikë për sigurinë e burimeve kryesore, si energjia elektrike, karburanti etj. c) Implemento masat e sigurisë sipas standarteve të industrisë për të mbrojtur burimet dhe pajisjet.	• Politikë e dokumentuar për të mbrojtur burimet kryesore, duke përshkruar lloje të ndryshme të burimeve dhe masat e sigurisë për të mbrojtur këto burime. • Evidencë e masave sipas standartit të industrisë për të garantuar sigurinë e burimeve për shembull ftohjen, ristartim automatic pas ndërprerjeve të energjisë, gjeneratorët, bateritë etj.
3	d) Implemento masat e sigurisë për të mbrojtur burimet. e) Rishiko dhe përditëso politikën dhe procedurat rregullisht, duke marrë në konsideratë ndryshimet dhe incidentet dhe ndryshimet e mëparshme.	• Evidencë e masave për sigurinë e burimeve, si ftohjen active, UP, sistemet backup të energjisë etj. • Politikë e përditësuar për sigurinë e burimeve dhe pajisjeve mbështetëse, rishiko komentet ose ndryshimet.

SO 11: Kontrolli i Aksesit në rrjet dhe sistemet e informacionit

Vendos dhe mirëmbaj një kontroll aksesi logjik të duhur për aksesin në rrjet dhe sistemet e informacionit.

	Masat e Sigurisë	Evidenca
1	a) Përdoruesit dhe sistemet kanë identifikim unik dhe autentikohen kur aksesojnë shërbimet ose sistemet. b) Implemento mekanizmin e duhur të kontrollit logjik për rrjetin dhe sistemet e informacionit për të lejuar	• Loget e aksesit tregojnë identifikues unik për përdoruesit dhe sistemet kur lejojnë ose mohojnë aksesin. • Përmbledhje e autentikimit dhe metodave të kontrollit të aksesit për sistemet dhe përdoruesit.

	vetëm kontrollin e autorizuar.	
2	c) Implemento politikë për mbrojtjen e aksesit në rrjet dhe sistemet e informacionit, duke adresuar rolet, të drejtat, përgjegjësitë dhe procedurat për vendosjen dhe revokimin e të drejtave të aksesit. d) Zgjidh mekanizma të duhur të autentikimit në varësi të tipit të aksesit. e) Monitoro aksesin në rrjet dhe sistemet e informacionit, vendos një process të miratimit të përjashtimeve dhe regjistrimit të thyerjeve të aksesit.	• Politikë e kontrollit të aksesit duke përfshirë përshkrimin e roleve, grupeve, të drejtave të aksesit, procedurat për dhënien dhe revokimin e aksesit. • Tipe të ndryshme të mekanizmave të autentikimit për lloje të ndryshme të aksesit. • Loge të shkeljes së politikës të kontrollit të aksesit dhe përjashtimet të miratuara nga oficeri i sigurisë.
3	f) Vlerëso efektivitetin e politikave të kontrollit të aksesit dhe procedurave dhe implemento kontrolle në mekanizmat e kontrollit të aksesit. g) Politika dhe mekanizmat të kontrollit të aksesit rishikohen dhe kur nevojitet ndryshohen.	• Raporte të testeve të sigurisë të mekanizmave të kontrollit të aksesit. • Mjete për zbulimin e përdorimit jonormal të sistemeve ose sjelljeve jonormale të sistemeve (sistemet e zbulimit të ndërhyrjeve dhe anomalive). • Loge të sistemeve të zbulimint të ndërhyrjeve dhe anomalive. • Përditësime të politikës të kontrollit të aksesit, rishiko komentet ose ndryshimet.

SO 12: Integriteti i Rrjetit dhe Sistemeve të Informacionit

Vendos dhe mirëmbaj integritetin e rrjetit dhe sistemeve të informacionit dhe mbroji nga viruset dhe nga programet e tjera të dëmshme që mund të ndryshojnë funksionalitetin e sistemeve.

	Masat e Sigurisë	Evidenca
1	a) Siguro që programet e rrjetit dhe sistemet e informacionit nuk janë deformuar ose ndryshuar, duke përdorur kontrollin e inputeve dhe fireëall-et. b) Siguro që të dhënat kritike të sigurisë si passëord-ët, sekretet, celsat privatë, nuk	• Programet dhe të dhënat në rrjet dhe sistemet e informacionit mbrohen nëpërmjet kontrollit të inputeve, fireëall-et, enkriptimi dhe nënshkrimi. • Të dhënat kryesore të sigurisë mbrohen me mekanizma të mbrojtjes si memorje të shpërndarë, enkriptim, hashing etj. • Sisteme të zbulimit të programeve të

	bëhën publike dhe as ndryshohen. c) Kontrollo për programme të dëmshme në rrjet dhe sistemet e informacionit.	dëmshme janë prezente dhe të përditësuara.
2	d) Implemento masa sigurie sipas standarteve të industrisë, duke ofruar mbrojtje në thellësi ndaj modifikimit të sistemeve.	• Dokumentim sesi mbrojtja e programeve dhe të dhënave në rrjet dhe sisteme informacioni implementohet. • Mjete për zbulimin e përdorimit jonormal të sistemeve ose sjelljeve jonormale të sistemeve (si sistemet e zbulimit të ndërhyrjeve dhe anomalive). • Loge të sistemeve të zbulimit të ndërhyrjeve dhe anomalive.
3	e) Vendos kontrolle të mbrojtjes së integritetit të sistemeve. f) Vlerëso dhe rishiko efektivitetin e masave për të mbrojtur integritetin e sistemeve.	• Kontrolle të përditësuara për të mbrojtur integritetin e sistemeve, si nënshkrimi i kodit, etj. • Dokumentim të procesit të kontrollit të logeve për sistemet e zbulimit të ndërhyrjeve dhe anomalive.

D4: Menaxhimi i Operacioneve

Fusha "Menaxhimi i Operacioneve" mbulon procedurat operacionale, menaxhimin e ndryshimit dhe menaxhimin e aseteve.

SO 13: Procedurat Operacionale

Vendos dhe mirëmbaj procedurat operacionale për funksionimin e rrjetave dhe sistemeve të informacionit kryesore nga personeli.

	Masat e Sigurisë	Evidenca
1	a) Vendos procedura operacionale dhe përgjegjësi për funksionimin e sistemeve kritike.	• Dokumentim të procedurave operacionale dhe përgjegjësive për rrjetin dhe sistemet e informacionit kryesore.
2	b) Implemento një politikë për funksionimin e sistemeve për të garantuar që sistemet kryesore funksionojnë dhe menaxhohen sipas procedurave të paracaktuara.	• Politikë e dokumentuar për funksionimin e sistemeve kritike, duke përfshirë një përmbledhje të rrjetit dhe sistemev të informacionit.
3	c) Rishiko dhe përditëso	• Politikë/procedurë të përditësuar për

	politikën/procedurat për funksionimin e sistemeve kritike, duke marrë në konsideratë incidentet dhe/ose ndryshimet.	sistemet kritike, rishiko komentet dhe/ose ndryshimet.

SO 14 :Ndryshimi i menaxhimit.

Krijimin e procedurave të menaxhimit të ndryshimit të rrjetit dhe sistemeve te informacionit kritike në mënyrë që të minimizohet mundësia e incidenteve që rezultojnë nga ndryshimet.

	Masat e Sigurise	Evidenca
1	a) Ndiqni procedurat e paracaktuara, kur bën ndryshime në sistemet kritike.	•Dokumentimi i ndryshimeve te procedurave te menaxhimit per sistemet kritike
2	b) Zbatimi i politikave / procedurave për menaxhimin e ndryshimeve, për të siguruar që ndryshimet e sistemeve kritike janë bërë gjithmonë duke ndjekur një mënyrë të paracaktuar. c) procedurat e menaxhimit të ndryshimit te dokumentit, dhe rekordet për secilen ndryshojnë sipas hapave të procedurës së ndjekur.	• Dokumentimi i ndryshimit i politikave të menaxhimit / procedurat e përfshira, sistemet nënshtrohen politikës, objektivat, rrokulliset përsëri procedurat, etj • Për çdo ndryshim, një raport është në dispozicion që përshkruan hapat dhe rezultat i ndryshimit
3	d) procedurat e menaxhimit të rishikimit dhe përditesimit ndryshojne rregullisht, duke marrë parasysh ndryshimet dhe incidentet e shkuara.	Proceduarat e menaxhimit te përditesimeve, të shqyrtojë komentet dhe / ose ndryshimi i logos.

SO: 15 Menaxhimi i burimeve

Vendosja dhe mirembajtja e procedurave te menaxhimit te burimeve dhe kontrolli i konfigurimit me qellim menaxhimin e gadishmerise te burimeve kritike dhe konfigurimi i rrjetit kritik dhe sistemit te informacionit.

	Masat e Sigurise	Evidenca
1	Menaxhimi i burimeve kritike dhe konfigurimi i sistemit kritik	• Lista e burimeve kritike dhe sistemit kritik
2	Implementimi i politikave / procedurave per menaxhimin e burimeve dhe kontrollin e konfigurimit.	• Politikat e dokumentura / procedurat per menaxhimin e aseteve , duke perfshire rregullat dhe pergjegjesite , burimeve dhe konfigurimet te cilat jane subject i politikave , objektivat e menaxhimit te aseteve
3	Rishikimi dhe perditesimi i herepashershem te politikave te menaxhimit te burimeve , bazuar ne ndryshimet dhe incidentet e shkuara	• Nje inventar burimesh ose inventare, te cilet permbajne burime kritike dhe varesine ndermjet aseteve • Nje inventar i kontrollit te konfigurimeve ose inventare , te cilet permbajne konfigurime te sistemit kritik. Perditesimin e politikave te menaxhimit / procedurave , rishikim te komenteve/ dhe / ose ndryshim i logs.

D5 : Menaxhimi i Incidenteve

Domain " Menaxhimi I incidenteve mbulon gjetjen e , pergjigjen e , raportimin e incidenteve dhe komunikimin ne lidhje me incidentet"

SO 16: Procedurat e menaxhimit te incidenteve

Vendosja dhe mirembajtja e procedurave per menaxhimin e incidenteve , dhe dergimi te personeli te duhur.

	Masat e Sigurise	Evidencat
1	a)Sigurimi qe personeli eshte ne gadishmeri dhe i pergatitur te menaxhoje dhe ti perballoje incidentet b)Te regjistroje incidentet kryesore	•Personeli te kuptoje si te veproje me incidentet dhe si ti pershkallezoje Inventarizimi i incidenteve kryesore dhe per incident, impaktin, shkakun veprimet e ndermarra , dhe mesimin e nxjerre
2	c)Implementimi i politikave/ procedurave per menaxhimin e incidenteve	•Politikat/ procedurat per menaxhimin e incidenteve , duke perfshire llojin e aksidentit qe mund te ndodhe , objektivat, rolin dhe pergjegjesite , pershkrim I detajuar, per tipin e incidentit, si ta menaxhojme incidentin, si te shkallzojme tek menaxheri etj
3	d)Investigimi i incidenteve kryesore dhe raportimi i tyre final, duke perfshire veprime te ndermarra dhe rekomandime per te zvogeluar incidente te ngjashme e)Vleresimi i politikave te menaxhimit te incidenteve / procedurave bazuar ne incidente te shkuara.	•Raporte individuale i perballimit te shumices se incidenteve Perditesimi i politikave te menaxhimit / procedurave , rishikim komentesh dhe/ ose ndryshim i logs.

SO 17 : Aftesia e zbulimit te incidenteve

Krijon dhe miremban aftesine e zbulimit te incidenteve qe zbulon incidente

	Masat e Sigurise	Evidenca
1	a) Ngritja e proceseve apo sistemeve për zbulimin e incidentit.	• Incidentet e meparshme janë zbuluar dhe dërguar në kohë tek njerëzit e duhur.
2	b) Implementimi i sistemeve standarde të industrisë dhe procedurat për zbulimin e incidentit. c) Implementimi i sistemeve dhe procedurave për regjistrimin dhe përcjellja incidente ne kohë te njerëzit e duhur.	Sistemet dhe procedurat e zbulimit te incidentit, të tilla si incidentet e Sigurise dhe për Menaxhimin e Ngjarjeve (SIEM) mjete, Helpdesk siguri për personelin, raportet dhe advisories nga kompjuteri Ekipet emergjente Përgjigje (certs), mjetet për vend anomali, e të tjera.

3	d)Rishikimi i Sistemeve dhe procesit për zbulimin e incidentit rregullisht dhe përditësimin e tyre duke marrë parasysh ndryshimet dhe incidenteve të fundit. .	• Perditesimin e dokumentacionit të sistemeve të zbulimit incidenteve dhe proceseve. • Dokumentimi i rishikimit të procesit të zbulimit të incidentit, të shqyrtojë komentet, dhe / ose ndryshim i logs.

SO 18: Raportimi i incidentit dhe komunikimi

Vendos dhe mirembaj procedurat e raportimit dhe komunikimit per incidentet perkatese,duke marrë në llogari legjislacionin kombëtar të autoriteteve qeveritare në incidentin e raportimit.

	Masat e Sigurise	Evidenca
1	a)Të komunikojnë dhe të raportojnë në lidhje të vazhdueshme ose incidente të fundit të palëve të treta, konsumatorët, dhe / ose autoritetet qeveritare, kur është e nevojshme.	• Evidenca te komunikimeve te shkuara dhe raportime te incidenteve
2	Implementon politika dhe procedura per komunikimin dhe raportimin ne lidhje me incidentet	• Politika dhe procedurat për komunikimin dhe raportimin në lidhje me incidentet, duke e përshkruar arsyeve / motivimet për të komunikuar apo raportim (arsyet e biznesit, arsyet ligjore etj), lloji i incidenteve në fushëveprimin, përmbajtjen e kërkuar e komunikimit, njoftime dhe raporte të dokumentuara, kanalet që do të përdoren , dhe rolet përgjegjëse për komunikimin, njoftuar dhe raportimin. • Modele për raportim dhe komunikim e incidentit
3	c) Vlerësoni komunikimet e shkuara dhe raportimin në lidhje me incidentet. d) Rishikimi dhe përditësimin e planeve të raportimit dhe komunikimit, bazuar në ndryshimet apo incidenteve të fundit.	• Lista e raporteve të incidenteve dhe të komunikimit të fundit në lidhje me incidentet • Deri në përgjigje të incidentit dhe politikës së komunikimit, të shqyrtojë komentet, dhe / ose ndryshim i logs.

D6: Menaxhimi i Vazhdimit të Biznesit

Domain "Menaxhimi i vazhdimit te Biznesit" mbulon vazhdimësinë e strategjitve dhe planeve te emergjences për te zbutur deshtimet e medha dhe /ose të fatkeqësive natyrore

SO 19: Strategjia e Vazhdimit të Shërbimit dhe Planet e Emergjencës

Të krijojë dhe mirëmbajë plane emergjente dhe një strategji për të siguruar vazhdimësinë e rrjeteve dhe shërbimeve të komunikimit të ofruara.

	Masat e Sigurise	Evidenca
1	a) Implemento një strategjie ne vazhdimësinë e shërbimi për rrjetet e komunikimeve dhe / ose shërbimeve të ofruara.	• Strategji te dokumentuar per vazhdimësinë e shërbimit, duke përfshirë objektivat kohë për shërbimet kryesore dhe proceseve.
2	a) Zbatimi plane rezervë për sistemet kritike. b) Aktivizimin i monitorimit dhe zbatimin e planeve të paparashikuara, regjistrimi herëve të suksesshme dhe të kohes se dështimit.	•Plane emergjence për sistemet kritike, duke përfshirë hapa te qarta dhe procedurat për kërcënimet e njohura, shkaktuesit për aktivizimin, hapat dhe objektivat kohore • Procesi i vendimit për aktivizimin e planeve të emergjente. • Shkrime të aktivizimit dhe të ekzekutimit të planeve emergjente, duke përfshirë vendimet e marra, hapat e ndjekur, koha e rregullimit final.
3	d) Rishikimi e sherbimeve strategjike ne menyre te vazhdueshme dhe periodikisht d) Rishikimin plane emergjence, bazuar në incidentet e fundit dhe ndryshimet.	• Perditesimi i strategjise ne vazhdueshmeri dhe planin e incidenteve, rishikim komentesh, dhe /ose ndryshim i logs.

SO 20: Kapacitetet per rimekembjen e katastrofave ne rrjet

Vendos dhe mirëmbajë e kapaciteteve te duhura per rimekembjen dhe rikthimin ne gjendje normale te rrjetit dhe sherbimeve te tjera te komunikimit ne rastet e katastrofave natyrale ose/dhe te me pasoja e medha.

	Masat e Sigurise	Evidenca
1	a) Pergatitja per rikthimin ne gjendje normale e sherbimeve ne katastrofen e rradhes	Permasat merren gjithmone ne lidhje me situaten, si p.sh failover ne zona te tjera pervec rrjetit akual qe po perdoret, backup I te dhenave kritike ne distanca te largeta etj.

2	b) Implementimi i proçedurave/policive per efektivitetin sa me te larte te kapaciteteve per rimekembjene e situates c) Implementimi I kapaciteteve te industrive standarte te rimekembjes se katastrofave ose te perdorin pale te treta (siç jane rrjetet emergjente nacionale)	Proçedurat/policite Documented policy/ per efektivitetin sa me te larte te kapaciteteve per rimekembjene e situates, duke perfshire nje liste te katastrofave natyrale qe mund ndikojne ne sherbime, dhe nje liste te kapaciteteve (ato nga palet e treta por edhe ato te brendshem) Implementimin e industrive standarte per kapacitetet e rimekembjes , siç jane pajisjet mobile, sitet mobile, sitet failover etj.
3	c) Vendosja e nje mekanizmi per mitigimin kapaciteteve per rregullimin e situates d) Kontrollimi dhe updatimi I kapacatiteve en menyre te vazhdueshme te regullt, duek amrre parasysh ndryshimet qe ndodhin, incidentet e meparshme, rezultatet e testeve.	Ky lloj mekanizmi perfshin te gjithe mekanizmat failover paandalues per katastrofat natyrale me pasoja te medha Dokumentimi i kapaciteteve per rregullimin e situates ne fjale , te shikohen komentet dhe/ ose ndryshim i logs.

D7: Monitorimi, Auditimi dhe Testimi

Domaini "Monitorimi, auditimi dhe testimi" mbulon monitorimin, testimin dhe auditimin e rrjetit dhe sistemeve informatike duke na dhene shume thjeshtime.

SO:21 Politikat e Logimit dhe Monitorimit

Vendos dhe mirëmbajë sistemet dhe funksionet për monitorimin dhe loggimin e rrjeteve kritike dhe sistemeve te komunikimit.

	Masat e Sigurise	Evidenca
1	a)Imlementimin e monitorimit dhe loggin e sistemeve kritike	•Logot dhe raportet e monitorimit të rrjetit kritik dhe të sistemeve te informacionit.
2	b) Implementon politikën e ngjarjeve dhe monitorimin e sistemeve kritike. c) Vendos mjete për monitorimin e sistemeve kritike d) Vendos mjetet për të mbledhur dhe ruajtur shkrimet e sistemeve kritike.	•Politika te dokumentuara për monitorimin dhe ngjarjet, duke përfshirë kerkesat minimale per monitorimin dhe ngjarjet, periudhën e mbajtjes, dhe objektivat e përgjithshme të ruajtjes monitoringdata dhe shkrimet. • Mjetet për sistemet e monitorimit dhe

		mbledhjen e logot
3	e) Vendos mjetet për mbledhjen dhe analizën e të dhënave të monitorimit dhe logot. f) Rishikimi dhe perditesimin i ndodhive dhe monitorimin e politikave / procedurave, duke marrë parasysh ndryshimet dhe incidenteve te shkuara.	•Mjete për të lehtësuar regjistrimin strukturor dhe analizën e monitorimit dhe logot. • Përditësuar dokumentacionin e monitorimit dhe politikat e ngjarjeve / procedurat, të shqyrtojë komentet, dhe / ose ndryshim i logs

SO:22 Ushtrimi i planeve emergjente

Vendos dhe mirëmban politika për testimin dhe ushtrimin backup dhe të planeve emergjente, ku nevojitet bashkëpunim me palët e treta.

	Masat e Sigurise	Evidenca
1	a) Veprime dhe backup provë dhe planet emergjente për t'u siguruar që sistemet dhe proceset e punës dhe personeli është i përgatitur për dështimet e mëdha dhe të paparashikuara.	•Raportet e veprimeve te fundit të backup dhe të planeve emergjente.
2	b)Implementimi i programit për ushtrimin backup dhe planeve emergjente rregullisht, duke përdorur skenare realiste që mbulojnë një gamë të skenarëve të ndryshëm gjatë kohës. c) Sigurohuni që çështjet dhe mësimet e nxjerra nga ushtrimet janë adresuar nga njerëzit përgjegjës dhe se proceset dhe sistemet përkatëse janë përditësuar në përputhje me rrethanat.	•Programet e veprimit per backup dhe plane emergjente duke perfshire llojet e papritura , frekuencën, rolet dhe përgjegjësitë, modelet dhe procedurat për kryerjen e ushtrimeve, modele për raportet e ushtrimit. • Raportet mbi ushtrimet dhe testimet tregon ekzekutimin e planeve emergjente, duke përfshirë mësimet e nxjerra nga ushtrimet. • Çështjet dhe mësimet e nxjerra nga ushtrimet e shkuara kanë qenë të drejtuar nga njerëzit përgjegjës.

3	d) Rishikimi dhe përditësimin e planeve te ushtrimit, duke marrë parasysh ndryshimet dhe incidentet e shkuara dhe të paparashikuara të cilat nuk janë të mbuluara nga programi i veprimit. d) Përfshirja furnizuesit, si dhe palët e tjera të treta, si partnerët e biznesit ose konsumatorët në veprim.	• Perditesimi i planeve te ushtrimit, të shqyrtojë komentet, dhe / ose të ndryshojë logot. • Input nga furnizuesit dhe palët e tjera të treat përfshira për mënyrën se si të përmirësojme skenarin e ushtrimeve.

SO 23: Rrjeti dhe testimi i sistemit te informacionit

Vendos dhe mirëmbajë rregulla për testimin e rrjetit dhe sistemet e informacionit, veçanërisht kur lidhja eshte me rrjete ose sisteme te reja.

	Masat e Sigurise	Evidenca
1	a)Testo rrjetet dhe sistemet e informacionit perpara se ti perdorni ato ose ti lidhni me sistemet egzistuese.	•Testo raportet e rrjetit dhe sistemeve te informacionit, duke perfshire testet pas ndryshimeve te medha ose prezantimit te sistemeve te reja.
2	b) Implemento rregulla dhe procedura per te testuar rrjetin dhe sitemet e informacionit, c)Implemento vegla per testime automatike	•Rregullat/procedurat per testimin e rrjeteve dhe sistemeve te informacionit, duke perfshire kur tested duhet te behen, planifikimi i testeve, rasted e testeve, tabela shembull boshe te rraporteve te testeve.
3	c)Rishikimi dhe azhurnimi i rregullave / procedurat për testim, duke marrë parasysh ndryshimet dhe incidentet e fundit.	•Lista e raporteve të testimit. • Rregullat /procedurat e permirsuara te reja për testimin e rrjeteve dhe sistemet e informacionit, të shqyrtojë komentet, dhe / ose dokumentin (logun) i ndryshimeve.

SO 24: Vleresimi i Sigurise

Vendosja dhe mirëmbajtja e përshtatshme e politikave për kryerjen e vlerësimeve të sigurisë të rrjetit dhe të sistemeve te informacionit.

	Masat e Sigurise	Evidenca

1	a) Siguro qe sistemet kritike tu nënshtrohen sigurisë se canimeve dhe testimin e sigurisë rregullisht, sidomos kur sistemet e reja janë futur dhe ndiqen ndryshimet. .	•Raporto nga scanimet e sigurise se meparshme dhe testet e sigurise.
2	b) Implemento rregulla/procedura për vlerësimin e sigurisë dhe testimin e sigurisë.	•Rregullat / Procedurat e dokumentuara për vlerësimin dhe testimin e sigurisë, duke përfshirë, cilat asete, në çfarë rrethanash, lloji i vlerësimeve të sigurisë dhe testet, frekuenca, palet e miratuara (të brendshme ose të jashtme), nivelet e konfidencialitetit për vlerësimin dhe rezultatet e testimit dhe vlerësimet e objektivave të sigurisë dhe testet.
3	c) Vlereso efektivitetin e politikave / procedurave për vlerësimin dhe testimin e sigurisë. d) Shqyrto dhe korrigjo politikat / procedurat për vlerësimin dhe testimin e sigurisë, duke marrë parasysh ndryshimet dhe incidenteve të shkuara.	•Lista e raporteve per vleresimin dhe testimin e sigurise. •Raportet e veprimive te ndermarra në vlerësimin dhe rezultatet e testimit •Ndrysho rregullat / procedurat për vlerësimin dhe testimin e sigurisë,shqyrto komentet, dhe / ose ndryshim i logs.

SO 25: Monitorimi i pajtueshmerise – Monitorimi i rregullt sipas ligjit

Vendosja dhe mirmbaje e politikave per monitorimin e pajtueshmerise me standarte dhe kerkesat ligjore.

	Masat e Sigurise	Evidenca
1	a) Monitoro zbatimin brenda standardeve dhe kërkesave ligjore	•Raporte qe pershkruajne rezultatin e zbatimit monitorimit
2	b) Implemento rregulla dhe procedura per monitorimin e rregullt dhe auditimin	•Rregullat / Procedurat e dokumentuara për monitorimin e zbatimit te rregullt dhe auditimit, duke përfshirë edhe (aktiveve, proceset, infrastruktura), frekuencat, udhëzimet që duhet të kryejnë auditime (te brendshme- ose të jashtme), rregullat përkatëse të sigurisë që janë objekt i monitorimit të pajtueshmërisë dhe auditimit, objektivat dhe synimet e nivel të lartë të

		monitorimit të pajtueshmërisë dhe auditimit, templeta(rregjistra) për raportet e auditimit. •Monitorime te detajuara dhe plane auditimi duke perfshire objektive dhe planifikim te nivelit te larte dhe afatgjate.
3	c)Vlerësoni politikat / procedurat sipas standarteve dhe auditim d) Rishikimi dhe perditesimi i politikave/ procedurat për pajtim dhe të auditimit, duke marrë parasysh ndryshimet dhe incidenteve të fundit.	•Lista e të gjitha raporteve dhe ankesave të pajtueshmërisë dhe auditimit •Rregullat e perditesuara/ procedurat e e ankuara dhe auditimin, shqyrtimi i komenteve, dhe / ose të ndryshimi te logos.