REPUBLIKA E SHQIPËRISË

AUTORITETI I KOMUNIKIMEVE ELEKTRONIKE DHE POSTARE

R R E G U LL O R E

“MBI MASAT ORGANIZATIVE DHE TEKNIKE PËR GARANTIMIN E SIGURISË SË RRJETEVE DHE SHËRBIMEVE TË KOMUNIKIMEVE ELEKTRONIKE”

Miratuar me Vendim të Këshillit Drejtues nr.8, datë 13.03.2026

RREGULLORE

"MBI MASAT ORGANIZATIVE DHE TEKNIKE PËR GARANTIMIN E SIGURISË SË RRJETEVE DHE SHËRBIMEVE TË KOMUNIKIMEVE ELEKTRONIKE"

Neni 1

Qëllimi

Kjo rregullore përcakton detyrimet e sipërmarrësve që operojnë për ofrimin e rrjeteve dhe/ose shërbimeve publike të komunikimeve elektronike, për marrjen e masave të duhura, teknike, operacionale dhe organizative, proporcionale me rreziqet që kërcënojnë sigurinë dhe integritetin e rrjeteve/shërbimeve. Masat e marra, duke pasur parasysh gjendjen bashkëkohore të teknologjisë, duhet të sigurojnë një nivel të përshtatshëm sigurie ndaj rreziqeve të identifikuara dhe në veçanti të parandalohet ose të minimizohet ndikimi i incidenteve të sigurisë tek përdoruesit dhe tek rrjetet/shërbimet e ndërlidhura.

Neni 2

Objekti

1. Rregullorja synon të përcaktojë:
    a. Objektivat dhe masat për garantimin e funksionimit të sigurt të infrastrukturës së rrjetit dhe/ose shërbimeve të komunikimeve elektronike, nga sipërmarrësit që ofrojnë akses në rrjetet dhe/ose shërbimet publike të komunikimeve elektronike, duke siguruar konfidencialitetin, integritetin dhe disponueshmërinë e vazhdueshme të këtyre rrjeteve/shërbimeve.
    b. Detyrimet dhe masat bazë që sipërmarrësit duhet të ndërmarrin për të parandaluar ndodhjen e incidenteve të sigurisë kibernetike në rrjetet dhe/ose shërbimet e komunikimeve elektronike, ose për të minimizuar pasojat e tyre, si dhe për t'i raportuar ato në mënyrë të rregullt kur ndodhin.
    c. Kushtet në bazë të të cilave një cenim apo incident sigurie konsiderohet i rëndësishëm, në mënyrë që të lind detyrimi i sipërmarrësit për të informuar AKEP dhe autoritetet e tjera kompetente në lidhje me këtë cenim ose incident sigurie.
    d. Standardizimin në vlerësimin dhe raportimin e incidenteve të sigurisë, dhe masave të sigurisë të ndërmarra nga sipërmarrësit, duke siguruar përdorimin e një metodologjie dhe formati unik raportimi, sipas modeleve të miratuara nga AKEP (Aneksi 1 dhe Aneksi 2).
    e. Mënyrën dhe përmbajtjen e raportimit periodik të masave të sigurisë dhe incidenteve të sigurisë, që duhen dorëzuar nga sipërmarrësit pranë AKEP.
    f. Masat administrative dhe sanksionet që zbatohen në rast se sipërmarrësit nuk përmbushin detyrimet e parashikuara në këtë rregullore, bazuar në nenin 184 të ligjit nr. 54/2024.

Neni 3

Fusha e zbatimit

Kjo rregullore zbatohet për të gjithë sipërmarrësit/operatorët që ofrojnë rrjete publike të komunikimeve elektronike, ose shërbime të komunikimeve elektronike të disponueshme për publikun, brenda territorit të Republikës së Shqipërisë. Detyrimet e kësaj rregulloreje zbatohen pavarësisht teknologjisë apo platformës së përdorur, duke përfshirë ofruesit e shërbimeve tradicionale të telefonisë dhe internetit, në masën e përcaktuar nga ligji, si dhe ofruesit e rrjeteve 5G.

Neni 4

Baza ligjore

1. Kjo rregullore është hartuar në zbatim të nenit 56 të ligjit nr. 54/2024 "Për komunikimet elektronike në Republikën e Shqipërisë"[1] si dhe mban parasysh detyrimet e përcaktuara në Kreun VII, nenin 54, 148 dhe 157 të ligjit nr. 54/2024, lidhur me sigurinë e rrjeteve dhe shërbimeve, disponueshmërinë e shërbimeve, marrjen e masave mbrojtëse teknike dhe organizative.
2. Rregullorja mban parasysh standardet e Direktivës së BE-së 2022/2555 (NIS2) e cila përfaqëson praktikën më të mirë evropiane në fushën e sigurisë kibernetike si dhe përcaktimet lidhur me mbrojtjen e të dhënave personale të pajtimtarëve, bazuar në legjislacionin në fuqi për të dhënat personale.

Neni 5

Përkufizime

Termat e përdorur në këtë Rregullore do të kenë të njëjtin kuptim si në ligjin nr. 54/2024 "Për komunikimet elektronike në Republikën e Shqipërisë".

Neni 6

Kriteret për vlerësimin e ndikimit të incidenteve të sigurisë

1. **Vlerësimi fillestar i impaktit:** Sipërmarrësit janë të detyruar të kryejnë sa më shpejt një vlerësim paraprak/fillestar të ndikimit të çdo incidenti sigurie mbi rrjetet dhe/ose shërbimet e tyre të komunikimeve elektronike publike. Ky vlerësim fillestar bazohet në kriteret e Aneksit 2 të kësaj rregulloreje, i cili parashikon një matricë të vlerësimit të impaktit sipas parametrave

[1] Ligji nr. 54/2024, është i përafruar me Direktivën e (BE) 2018/1972 të Parlamentit Evropian dhe Këshillit , datë 11 dhjetor 2018 "Për krijimin e Kodit Evropian të Komunikimeve Elektronike".

kryesorë si: ndikimi në shërbime kritike, kohëzgjatja e ndërprerjes, numri i përdoruesve të prekur, shtrirja gjeografike e ndikimit, impakti social-ekonomik i incidentit, etj.

Klasifikimi i incidentit si me impakt të "ulët", "mesatar" ose "të lartë", bëhet duke iu referuar pragjeve të përcaktuara në Aneksin 2.

2. **Klasifikimi i incidenteve:** Në përfundim të vlerësimit fillestar, nëse sipas Aneksit 2, incidenti klasifikohet me impakt "mesatar" ose "të lartë, atëherë sipërmarrësit kanë detyrimin për të njoftuar në AKEP.
3. **Rivlerësimi dhe vlerësimi përfundimtar:** Sipërmarrësit duhet të përditësojnë vlerësimin e impaktit sa herë që dalin të dhëna ose analiza të reja mbi incidentin. Brenda 30 (tridhjetë) ditëve kalendarike nga ndodhja e incidentit të sigurisë, sipërmarrësi dorëzojnë në AKEP, një vlerësim përfundimtar të impaktit, i cili përfshin të dhënat e verifikuara, analizën e plotë të shkakut/eve dhe masat e marra për reduktimin e pasojave. Ky raport përfundimtar do të përgatitet sipas formatit të Aneksit 1 dhe 2 dhe do të shërbejë si bazë për përmirësime të mundshme të masave të sigurisë nga ana e operatorit.

Neni 7

Masat për rritjen e sigurisë së rrjeteve dhe shërbimeve

1. **Masa organizative dhe plane operacionalë:** Me qëllim parandalimin e incidenteve të sigurisë dhe minimizimin e ndikimit të tyre, sipërmarrësit e rrjeteve dhe shërbimeve publike të komunikimeve elektronike, janë të detyruar të ndërmarrin masat organizative të mëposhtme:

    a. **Miratimin e një politike të brendshme të sigurisë së informacionit**, nga stafi drejtues i sipërmarrjes. Politika duhet të jetë e shkruar, e publikuar nga sipërmarrësi dhe të komunikohet tek i gjithë personeli, dhe të rishikohet e rifreskohet rregullisht (jo më rallë se 1 (një) herë në vit ose pas çdo incidenti të rëndësishëm sigurie apo ndryshimi madhor në infrastrukturë). Kjo politikë përfshin objektivat kryesorë të sigurisë, fushën e zbatimit (për sistemet, pajisjet dhe të dhënat që mbulon), si dhe parimet bazë që duhet të respektohen (p.sh. parimi i sigurisë në shtresa, parimi i privatësisë në projektim, etj).

    b. **Menaxhimin e rrezikut kibernetik:** Të krijojnë dhe zbatojnë një kuadër të dokumentuar për menaxhimin e rrezikut të sigurisë kibernetike, që synon identifikimin, vlerësimin dhe trajtimin sistematik të rreziqeve ndaj rrjeteve dhe sistemeve të informacionit. Kjo përfshin: metodologjinë e menaxhimit të rrezikut (p.sh. standardet e ndjekura, kriteret e vlerësimit), hartimin e një regjistri rreziqesh me rreziqet kryesore të identifikuara (duke përfshirë kërcënimet e brendshme dhe të jashtme, si dhe rreziqet nga palë të treta/furnizuesit), prioritizimin e rreziqeve sipas niveleve të tyre, dhe planin e trajtimit të tyre (përmes evitimit, zmbrapsjes, transferimit ose pranimit të rrezikut).

    Ky proces duhet të jetë i vazhdueshëm: të rishikohet të paktën 1 (një) herë në vit dhe menjëherë pas çdo incidenti të rëndësishëm ose ndryshimi madhor në sisteme.

c. **Strukturë organizative e sigurisë dhe përgjegjësitë:** Të caktojnë qartë rolet dhe përgjegjësitë për menaxhimin e sigurisë së informacionit brenda sipërmarrësit. Kjo nënkupton:
   i. emërimin e të paktën një personi të autorizuar, në nivel të duhur menaxherial, përgjegjës për çështjet e sigurisë kibernetike, i cili do të veprojë edhe si pikë kontakti me AKEP, për incidentet dhe raportimet e sigurisë;
   ii. përcaktimin e roleve të tjera kyçe (p.sh. administratorë sistemi, oficerë të sigurisë fizike, oficerë/nëpunës të mbrojtjes së të dhënave personale (DPO), etj.) dhe detyrat e secilit lidhur me sigurinë;
   iii. formalizimin e këtyre përgjegjësive në organigramën e sipërmarrësit dhe në përshkrimet e punës.

d. **Trajnimi dhe ndërgjegjësimi i personelit:** Të ndërmarrin programe të rregullta trajnimi kibernetik dhe fushata ndërgjegjësimi për të gjithë punonjësit, veçanërisht për ata që kanë role në sigurinë e informacionit ose që operojnë sisteme kritike. Programi i trajnimit duhet të përfshijë temat bazë të sigurisë (si politika e sigurisë së kompanisë, njohuri mbi phishing/uniformitetin, menaxhimi i fjalëkalimeve, procedurat e raportimit të incidenteve) dhe të zgjerohet sipas rolit (p.sh. trajnime teknike të avancuara për administratorët e rrjetit). Të paktën 1 (një) herë në vit duhet të kryhet një seancë e detyrueshme trajnimi për të gjithë stafin, si dhe trajnime shtesë pas incidentesh ose kur identifikohen dobësi në njohuritë e stafit.

e. **Politikat e përdorimit të log-eve dhe mbrojtja e të dhënave personale:** Të hartojnë politika të qarta për monitorimin e sistemeve dhe përdorimin e log-eve, në mënyrë transparente ndaj punonjësve dhe pajtimtarëve, për aq sa këto log-e mund të përbëjnë të dhëna personale. Përdoruesit/pajtimtarët dhe punonjësit duhet të informohen qartë dhe lehtësisht mbi çfarë të dhënash personale mund të përpunohen në kuadër të masave të sigurisë së rrjeteve (p.sh. log-et e trafikut, monitorimi i komunikimeve, sistemet e zbulimit të intruzioneve etj.). Gjithashtu, sipërmarrësi duhet të ketë një politikë të ruajtjes së të dhënave personale të përftuara nga këto masa sigurie, ku të përcaktohen dhe dokumentohen afatet e ruajtjes së log-eve dhe të dhënave të tjera, në përputhje me parimin e kufizimit të periudhës së ruajtjes.

f. **Planifikimi i vazhdimësisë së shërbimit dhe rimëkëmbjes:** Të përgatisin dhe implementojnë një Plan të Vazhdimësisë së Veprimtarisë (BCP) dhe planin e Rimëkëmbjes nga Fatkeqësitë (DRP), i cili aktivizohet menjëherë në rast incidenti sigurie madhor. Plani i vazhdimësisë duhet të identifikojë shërbimet dhe proceset kritike, të përcaktojë strategjitë për vazhdimin e funksionimit të tyre edhe nën kushte të degradimit (p.sh. përdorimi i sistemeve rezervë, devijimi i trafikut në rrjete alternative) dhe të caktojë ekipet/rolet përgjegjëse për secilin skenar emergjent. Plani i rimëkëmbjes duhet të detajojë procedurat për rikthimin e sistemeve në gjendje normale pas një avarie apo sulmi (p.sh. restaurimi i backup-eve, rindërtimi i serverave, **disaster recovery site**, etj.). Këto plane duhet të testohen periodikisht (p.sh. me ushtrime ose simulime vjetore) për të siguruar efektivitetin e tyre. *(dokumenti i BCP/DRP i miratuar; rezultatet dhe raportet e testeve të vazhdimësisë/rimëkëmbjes; lista e sistemeve kritike dhe RTO/RPO për secilin prej tyre.)*

g. **Siguria e zinxhirit të furnizimit (supply chain security):** Operatorët duhet të zhvillojnë politika dhe të marrin masa konkrete për të siguruar që furnizuesit dhe partnerët e tyre teknikë të përmbushin kërkesat e sigurisë kibernetike. Kjo përfshin:
   i. **vlerësimin e rrezikut të furnitorëve kryesorë** të pajisjeve dhe shërbimeve (p.sh. furnizuesit e pajisjeve të rrjetit 5G, ofruesit e shërbimeve cloud që përdoren nga operatori, etj.) duke marrë parasysh elemente si: praktikat e tyre të sigurisë, vendin e origjinës, certifikimet e sigurisë kibernetike (p.sh. ISO 27001, certifikime në kuadër të skemave evropiane), historikun e incidenteve të njohura dhe vlerësimet kombëtare/evropiane të riskut për ta;
   ii. **kërkesat kontraktuale të sigurisë**: siguria duhet të përfshihet në kontratat me palët e treta (p.sh. detyrimi i tyre për të njoftuar operatorin për incidente që ndikojnë në shërbimin e ofruar, zbatimi nga ana e tyre i standardeve minimale, si dhe lejimi i auditimeve nga operatori ose autoritetet);
   iii. **kontrollet e zinxhirit të furnizimit**: operatori duhet të aplikojë kontrolle teknike për të mbrojtur sistemet e veta nga dobësitë e furnitorëve (p.sh. monitorim i veçantë i pajisjeve/aplikacioneve të furnizuara, segmentim i rrjetit për pajisjet e palëve të treta, verifikim i integritetit të përditësimeve që vijnë nga furnitori, etj.) Në rastin e rrjeteve 5G, operatori duhet të respektojë masat e miratuara nga autoritetet kombëtare në kuadër të EU 5G Toolbox, të mos përdorë pajisje nga furnizues të konsideruar me risk të lartë në pjesët kritike të rrjetit, sipas listës së miratuar me vendim të Këshillit të Ministrave, për këtë qëllim.
   iv. **Kontrolli i aksesit dhe menaxhimi i identiteteve:** (Ndërthur elemente teknike e organizative). Operatori duhet të vendosi politika strikte për menaxhimin e llogarive dhe aksesit në sistemet e tyre. Kjo përfshin parimin e aksesit minimal (çdo përdorues ose proces të ketë vetëm aksesin e nevojshëm për detyrën e tij), menaxhimin e kredencialeve (fjalëkalime të forta, rotacion periodik, ndalim i përdorimit të llogarive të përbashkëta pa emër), përdorimin e autentifikimit me shumë faktorë, kudo ku është e mundur, veçanërisht për akseset e privilegjuara dhe mjetet e administrimit, dhe monitorimin e vazhdueshëm të log-eve të aksesit, për të zbuluar përdorime të paautorizuara).

2. **Masat teknike dhe operacionale:** Krahas masave organizative të mësipërme, sipërmarrësit janë të detyruar të implementojnë masat e detajuara teknike dhe operative të përcaktuara në Aneksin 3, që i bashkëngjitet kësaj rregulloreje. Aneksi 3 përfshin objektivat specifikë të sigurisë kibernetike dhe masat minimale që duhen zbatuar në fusha si: siguria fizike e infrastrukturës, kontrolli i aksesit logjik, përdorimi i pajisjeve kriptografike dhe enkriptimi, zbulimi dhe reagimi ndaj incidenteve, monitorimi i ngjarjeve dhe ruajtja e log-eve, integriteti i sistemeve (mbrojtja ndaj malëare), menaxhimi i vazhdueshëm i azhurnimeve/dobësive, etj. Operatorët duhet të zbatojnë masat e Aneksit 3 si minimumin e detyrueshëm, dhe të synojnë nivelet më të larta të sigurisë kur kapacitetet teknike dhe burimet e tyre e lejojnë (parimi i përmirësimit të vazhdueshëm).
3. **Mbrojtja e të dhënave personale të përdoruesve:** Në zbatim të parimit të "sigurisë së përpunimit" të të dhënave personale, sipërmarrësit janë të detyruar të marrin masat

mbrojtëse lidhur me të dhënat personale të përdoruesve duke zbatuar parimin e aksesit minimal, në mënyrë që:

a. Të jenë të aksesueshme vetëm nga personeli i autorizuar, për qëllime specifike ligjore e të përcaktuara qartë (parimi "need-to-know"). Kjo lidhet me kontrollin e aksesit, trajtimin konfidencial të informacionit dhe nënshkrimin e marrëveshjeve për konfidencialitetin nga personeli.
b. Të mbrohen nga shkatërrimi, humbja, ndryshimi, zbulimi ose qasja e paautorizuar, aksidentale ose e paligjshme (integriteti dhe konfidencialiteti). Kjo nënkupton përdorimin e enkriptimit gjatë ruajtjes dhe transmetimit të të dhënave sensitive përdorimin e pseudonimizimit ose anonimizimit aty ku është e mundur, si dhe kopje rezervë të siguruara.
c. Të përpunohen sipas parimit "privacy by design and by default" – p.sh. në zhvillimin ose adoptimin e sistemeve të reja, siguria dhe mbrojtja e privatësisë të jenë të integruara që në fazën e projektimit. Kërkesat e kësaj pike vijnë në zbatim të legjislacionit për mbrojtjen e të dhënave personale, konkretisht me nenin 23 (Privacy by design/default) dhe nenin 28 (siguria e përpunimit) të këtij ligji.

Neni 8

Detyrimet e sipërmarrësve për njoftim

1. Njoftimi në AKEP, për incidentet e sigurisë: Sipërmarrësit kanë detyrimin të njoftojnë menjëherë AKEP dhe autoritetin kombëtar përgjegjës për sigurinë kibernetike (AKSK) për çdo incident sigurie të ndodhur, i cili klasifikohet me impakt të "mesatar" ose "lartë", sipas Aneksit 2. Njoftimi pranë AKEP, kryhet pa vonesa të panevojshme, në përputhje me përcaktimet e nenit 11 të kësaj rregulloreje.
2. Incidentet e sigurisë që janë objekt njoftimi sipas pikës 1, të këtij neni, mund të manifestohen në forma të ndryshme, duke përfshirë por pa u kufizuar në:

   a. Mohimi i marrjes së shërbimit (DoS/DDoS): sulme apo ngjarje që shkaktojnë mbingarkim të rrjetit apo sistemeve dhe pamundësojnë ofrimin normal të shërbimit te përdoruesit.
   b. Kompromet imi i sistemeve të informacionit: qasje e paautorizuar ose kompromet im (hakerim) i serverëve, rrjeteve apo bazave të të dhënave të operatorit, që cenon integritetin, konfidencialitetin apo disponueshmërinë e tyre.
   c. Ndërhyrje e paautorizuar e të dhënave elektronike: ndryshim, fshirje apo futje e të dhënave në sistemet e operatorit pa autorizim, duke shkaktuar dëm në shërbim (p.sh. manipulimi i konfigurimeve të rrjetit, injektimi i kodeve të dëmshme, etj.).
   d. Softwer i dëmshëm (malware), në pajisjet që janë nën kontrollin e drejtpërdrejtë të sipërmarrësit – infektimi me viruse, spyware, ransomware apo forma të tjera malware të sistemeve të operatorit, pavarësisht se mund të ketë ndodhur si pasojë e veprimeve të palëve të treta.
   e. Dështim i rëndë teknik, që shkakton ndikim në shërbime sipas kriterit të pikës 1, të këtij neni.

3. Sipërmarrësi ka detyrimin të njoftojë pajtimtarët e prekur dhe/ose të rrezikuar, kur:
    a. **Ekziston një kërcënim kibernetik i afërt ndaj përdoruesve**, i cili mund të ndikojë shërbimin që ata marrin (p.sh. një sulm i madh malware që përhapet shpejt dhe mund të prekë pajisjet e përdoruesve). Në këto raste operatori duhet t'u komunikojë përdoruesve masat ose veprimet që ata mund të ndërmarrin për të reduktuar rrezikun, p.sh. udhëzime për përditësimin e softwerit, ndryshimin e fjalëkalimeve, mos hapjen e mesazheve të dyshimta, etj. Nëse adresimi i këtyre masave kërkon kosto (p.sh. instalimi i një antivirusi të caktuar), operatori duhet të informojë përdoruesit se kush duhet të mbulojë këto kosto (nëse rreziku vjen jashtë kontrollit të operatorit, kostoja mund t'u bjerë vetë përdoruesve).
    b. **Ka ndodhur një cenim i të dhënave personale**. Në këto raste sipërmarrësi, përveç njoftimit që bën pranë Zyrës së Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, brenda 72 orësh, duhet t'i njoftojë vetë pajtimtarët e prekur, kur cenimi mund t'u shkaktojë atyre dëm (p.sh. vjedhja e kredencialeve, e të dhënave financiare apo informacioneve sensitive). Njoftimi për pajtimtarët duhet të përshkruajë në mënyrë të qartë natyrën e cenimit të të dhënave personale, pasojat e mundshme, masat e marra nga operatori dhe këshilla për pajtimtarin për mbrojtjen e mëtejshme (ndryshimi i fjalëkalimit, kontaktimi me bankën bllokimi i kartës, etj.). Gjithashtu, operatori duhet të bëj me dijeni pajtimtarët për pikën e kontaktit (adresë elektronike) të nëpunësit përgjegjës të mbrojtjes së të dhënave personale, në mënyrë që pajtimari të ketë një informacion sa më të detajuar.

4. Njoftimi i pajtimtarëve/përdoruesve për rreziqet: AKEP, nëse pas vlerësimit tërësor të incidentit të sigurisë me impakt të lartë të raportuar nga sipërmarrësi i rrjeteve dhe shërbimeve të komunikimeve elektronike, arrin në konkluzionin se ka një rezik të veçantë, i kërkon sipërmarrësit të njoftojë në mënyrë të menjëhershme pajtimtarët.
5. Përmbajtja e njoftimit për pajtimtarët: Njoftimi që u bëhet pajtimtarëve, duhet të hartohet në gjuhë të qartë e të thjeshtë dhe të përfshijë të paktën:
    i. një përshkrim të natyrës së cenimit të të dhënave personale;
    ii. adresën elektronike që mbulon pozicionin e nëpunësit të mbrojtjes së të dhënave personale pranë sipërmarrësi;
    iii. përshkrimin e masave që ka marrë ose propozon sipërmarrësi për të adresuar cenimin;
    iv. këshilla praktike për pajtimtarin në mënyrë që të zvogëlojë rreziqet (p.sh. ndryshimi i fjalëkalimeve, kujdes nga email-et e dyshimta – në varësi të llojit të cenimit). Këto informacione synojnë t'i japin pajtimtarit një pasqyrë sa më të plotë, në mënyrë që ai të ndërmarrë veprimet e duhura për mbrojtjen ndaj rrezikut.
6. **Detyrimi për njoftim me urdhër të AKEP:** Në rast se sipërmarrësi nuk arrin (ose vendos) të njoftojë pajtimtarët për një cenim serioz të të dhënave personale, AKEP, bazuar edhe në vlerësimin e ndikimit të cenimit, i kërkon zyrtarisht sipërmarrësit që të përmbushë detyrimin e njoftimit të pajtimtarëve. Kjo dispozitë siguron që pajtimtarët të mos mbeten pa informuar në raste cenimesh serioze, edhe nëse sipërmarrësi heziton ose vlerëson ndryshe. Kërkesa e AKEP, do të specifikojë dhe afatin brenda të cilit operatori duhet të kryejë njoftimin.

7. **Regjistri i shkeljeve të të dhënave personale:** Sipërmarrësit duhet të mbajnë një regjistër të brendshëm lidhur me çdo shkelje të sigurisë së të dhënave personale. Ky regjistër duhet të dokumentojë faktet rreth shkeljes, efektet e saj dhe masat korrigjuese të ndërmarra. Qëllimi i tij është që autoritetet kompetente (AKEP apo Zyra e Komisionerit, të mund të verifikojnë pajtueshmërinë e sipërmarrësit me detyrimin e njoftimit dhe masat e marra nga ana e tij.
8. **Njoftimi i ndërprerjeve/kufizimeve të shërbimit:**

    a. Sipërmarrësit duhet të informojnë AKEP, për kufizimin ose ndërprerjet e shërbimit:
        i. të paktën 48 orë përpara, në rastin e punimeve të planifikuara për përmirësimin, modernizimin ose mirëmbajtjen e rrjetit, që do të zgjasin më shumë se 30 minuta;
        i. sa më shpejt të jetë e mundur, por në asnjë rast më vonë se 48 orë pas ndodhjes së kufizimit ose ndërprerjes së shkaktuar nga defekte ose dëmtime të rrjetit, kur ndërprerja apo kufizimi impakton njëherazi një numër të konsiderueshëm përdoruesish që vlerësohet me impakt të mesëm ose të lartë, sipas Aneksit 2 të kësaj Rregulloreje.
    b. Sipërmarrësit duhet të njoftojnë për kufizimin ose ndërprerjet e shërbimit, pajtimtarët e prekur:
        ii. të paktën 48 orë përpara, në rastin e punimeve të planifikuara për përmirësimin, modernizimin ose mirëmbajtjen e rrjetit, që do të zgjasin më shumë se 30 minuta;
        iii. sa më shpejt të jetë e mundur, por në asnjë rast më vonë se 48 orë pas ndodhjes së kufizimit ose ndërprerjes së shkaktuar nga defekte ose dëmtime të rrjetit fiks, kur ndërprerja apo kufizimi impakton njëherazi një numër të konsiderueshëm përdoruesish që vlerësohet me impakt të lartë, sipas Aneksit 2 të kësaj Rregulloreje.
        iv. Për shkak të natyrës së shërbimit në rrjetin mobile dhe vështirësive objektive në identifikimin individual të abonentëve të prekur, njoftimi i pajtimtarëve sipas pikës 7/b/, të këtij neni, do të kryhet në përmbushje të parimit “best effort”.
9. **Sigurimi i informacionit dhe auditimeve me kërkesë të AKEP:** Me kërkesë të AKEP, sipërmarrësit janë të detyruar të:
    a. ofrojnë informacionin e nevojshëm të kërkuar nga AKEP për të vlerësuar sigurinë dhe integritetin e shërbimeve dhe rrjeteve të tyre. Kjo përfshin dërgimin e politikave të dokumentuara të sigurisë, rezultatet e vlerësimeve të rrezikut, listën e masave të zbatuara, konfigurimet kryesore të sigurisë, etj., sipas natyrës së informacionit që kërkohet.
    b. vënë në dispozicion rezultatet e auditimeve të sigurisë të kryera nga një organ i pavarur dhe i certifikuar, ose nga organi kompetent shtetëror për sigurinë kibernetike, për sistemet dhe rrjetet e tyre. Nëse një operator ka kryer auditime të jashtme, raportet përkatëse duhet t’i dorëzohen AKEP. Për më tepër, operatori duhet të lehtësojë kryerjen e auditimeve të jashtme të iniciuara nga vetë AKEP ose autoriteti kombëtar kibernetik, duke u dhënë akses audituesve në dokumentacion dhe në sisteme, brenda kufijve ligjorë. Kostoja e auditimeve të sigurisë mbulohet nga vetë sipërmarrësi, sipas nenit 56 të ligjit nr. 54/2024.

10. **Masa të urdhëruara nga AKEP** pas incidenteve/auditimeve: Në rast se ndodh një shkelje serioze e sigurisë, ose kur rezultatet e një auditi (sipas pikës 9/b) tregojnë se operatori nuk ka marrë masat e mjaftueshme të sigurisë, AKEP, me vendim, përcakton masat plotësuese dhe afatet kohore brenda të cilave sipërmarrësi duhet t'i zbatojë ato masa. Këto masa do të bazohen në kërkesat minimale të sigurisë të parashikuara në Aneksin 3, të kësaj rregulloreje dhe mund të përfshijnë: përmirësime teknike (p.sh. segmentimi i mëtejshëm i rrjetit, instalimi i sistemeve shtesë të zbulimit të ndërhyrjeve), rritje të burimeve njerëzore (p.sh. punësimi i ekspertëve të sigurisë), trajnime specifike, apo edhe kufizime operacionale deri në rregullimin e shkeljeve. Vendimi i AKEP, do të jetë i arsyetuar dhe do të përcaktojë afate realiste për përmbushjen e detyrimeve të reja nga sipërmarrësi.

Neni 9
Detyrimet e AKEP

1. Në kuadër të mbrojtjes së interesave të sigurisë kombëtare dhe garantimit të integritetit e sigurisë së rrjeteve publike të komunikimeve elektronike, AKEP, përmbush detyrimet si më poshtë:
   a. **Koordinimi me autoritetin kombëtar kibernetik:** AKEP informon pa vonesë autoritetin përgjegjës për sigurinë kibernetike në Republikën e Shqipërisë, për të gjitha incidentet e sigurisë kibernetike që i raportohen dhe që mund të kenë ndikim të rëndësishëm (sipas kritereve të nenit 6). Kjo mundëson një qasje të unifikuar kombëtare në menaxhimin e incidenteve madhore. Sipas rastit (p.sh. incidente me ndikim ndërkufitar ose që prekin edhe shtete të tjera), AKEP, informon gjithashtu Komisionin Evropian dhe ENISA, në përputhje me dispozitat ligjore për mbrojtjen e të dhënave gjatë transferimeve ndërkombëtare.
   b. **Informimi i publikut:** Kur AKEP konstaton se zbulimi publik i një incidenti të sigurisë është në interes të publikut (p.sh. për të rritur ndërgjegjësimin ose për të parandaluar përhapjen e mëtejshme të efektit), informon publikun vetë ose u kërkon sipërmarrësve ta bëjnë këtë. Praktikisht, kjo mund të realizohet duke lëshuar njoftime publike përmes medias, portalit zyrtar, rrjeteve sociale, etj., ose duke i udhëzuar operatorët që ata vetë t'u çojnë njoftime abonentëve të tyre apo publikut. Përpara se të publikohet informacioni, AKEP do të konsultohet me operatorin e prekur për t'u siguruar që njoftimi nuk zbulon të dhëna që do cënonin sigurinë e mëtejshme apo sekretet tregtare.
   c. **Shkëmbimi ndërkombëtar i informacionit:** AKEP shkëmben informacione në lidhje me shkeljet e sigurisë me Komisionin Evropian, ENISA, si dhe me autoritetet homologe të vendeve të tjera (veçanërisht atyre evropiane), kur është e nevojshme. Kjo bëhet në përputhje me kërkesat e NIS Cooperation Group dhe mekanizmave të tjerë ndërkombëtarë ku Shqipëria merr pjesë. AKEP kujdeset që gjatë këtij shkëmbimi të respektohen kufizimet ligjore për konfidencialitetin e informacionit dhe mbrojtjen e të dhënave personale. Informacioni që ndahet mund të përfshijë natyrën e incidentit, masat e marra, por jo detaje që identifikojnë individë apo sekrete tregtie, përveç

rasteve kur kërkohet ndryshe me ligj dhe me marrjen e masave mbrojtëse (p.sh. marrëveshje konfidencialiteti mes autoriteteve).

d. **Njoftimi i Zyrës së Komisionerit për të Dhënat Personale:** AKEP njofton menjëherë Zyrën e Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, në rastet kur një incident i sigurisë së rrjetit shoqërohet me cenim të të dhënave personale. AKEP, bashkëpunon ngushtë me këtë autoritet për të siguruar që sipërmarrësit kanë zbatuar politikat e sigurisë lidhur me përpunimin e të dhënave personale dhe kanë përmbushur detyrimet e njoftimit të subjekteve të këtyre tw dhënave. Ky koordinim siguron që aspektet teknike dhe ato të privatësisë të incidentit trajtohen në mënyrë të sinkronizuar.

2. Pikat nga a–d, të këtij neni, vijnë në harmoni me rolin mbikëqyrës të AKEP, sipas nenit 56 të ligjit për komunikimet elektronike dhe me praktikat më të mira evropiane për autoritetet rregullatore në sektorin e komunikimeve elektronike.

Neni 10

Raportimi i masave të sigurisë dhe auditimit

1. **Raportimi vjetor i masave të sigurisë:** Sipërmarrësit e komunikimeve elektronike janë të detyruar të paraqesin pranë AKEP, 1 (një) herë në vit, një raport gjithëpërfshirës mbi masat e sigurisë së zbatuara dhe gjendjen e sigurisë së rrjeteve e shërbimeve të tyre. Ky raport vjetor duhet të dorëzohet jo më vonë se muaji Shkurt i çdo viti (duke mbuluar vitin kalendarik pararendës) dhe të hartohet sipas formatit të përcaktuar në Aneksin 3 të kësaj rregulloreje.
2. **Kërkesa për raport auditimi të pavarur:** Sipërmarrësit e komunikimeve elektronike që plotësojnë një nga kushtet e mëposhtme:

    a. Kanë realizuar të ardhura vjetore nga komunikimet elektronike mbi 50,000,000 (pesëdhjetë milion) lekë;
    b. Kanë kontrata shërbimi me një ose disa institucione ose organizata të qeverisjes qendrore ose lokale;
    c. Kanë më shumë se 2000 (dymijë) abonentë
    d. Kanë linja interkoneksioni të internetit, pra sjellin internet me shumicë në Shqipëri

    kanë detyrimin të depozitojnë në AKEP, një nga dokumentet e mëposhtëm:

    i. Certifikatë ISO 27001, të shoqëruar nga Raporti i Auditimit Certifikues, i kryer nga një organ i pavarur i certifikuar ;
    ii. Raportin e Auditimit të Sigurisë të kryer nga autoriteti kompetent shtetëror për sigurinë kibernetike.

Përballimi i kostove të auditimit: Kostoja e auditimit të sigurisë, përballohet nga vetë sipërmarrësi në çdo rast. Sipërmarrësi duhet të kontraktojë me shpenzimet e veta një auditor të kualifikuar (p.sh. një shoqëri audituese me eksperiencë në fushën e sigurisë kibernetike), ose t'i lejojë autoritetit kompetent shtetëror (p.sh. ekipit të auditimit të

AKSK) kryerjen e auditimit me kosto që mund t'i faturohet sipërmarrësit sipas legjislacionit.

3. **Masa korrigjuese pas auditimit:** Në rast se nga auditimi rezulton se incidenti i sigurisë ka ndodhur për shkak të dobësive strukturore në sistemet e operatorit, dhe/ose raporti i auditimit nxjerr në pah masa të pamjaftueshme sigurie, AKEP , pas konsultimit me autoritetin kombëtar kibernetik, me vendim detyron sipërmarrësin të zbatojë masat e sigurisë shtesë, duke përcaktuar kërkesat minimale që duhen përmbushur referuar Aneksit 3 si dhe afatet konkrete për zbatimin e tyre. AKEP do të monitorojë nga afër përmbushjen e këtyre masave dhe mund të kërkojë prova periodike të progresit nga ana e operatorit.
4. **Privatësia gjatë auditimit:** Gjatë procesit të auditimit të sigurisë (qoftë të brendshëm apo të jashtëm), sipërmarrësit janë të detyruar të garantojnë pseudonimizimin ose anonimizimin e të dhënave personale, për të shmangur ekspozimin e panevojshëm të informacionit të identifikueshëm, në përputhje me parimet e mbrojtjes së të dhënave personale, në nenin 23 "Mbrojtja e të dhënave që në projektim dhe parazgjedhje" (*privacy by design and by default*) dhe nenin 28 "Masat për të garantuar sigurinë e përpunimit" të ligjit për mbrojtjen e të dhënave personale). Kjo do të thotë se audituesit duhet sa të jetë e mundur, të punojnë me log-e apo dataset të pastruara nga të dhënat e ndjeshme, përveç rasteve kur analizimi i tyre i plotë, është i domosdoshëm për vlerësimin e sigurisë. Edhe në rastet kur të dhënat personale duhen shqyrtuar, audituesit lidhen me detyrimin e konfidencialitetit dhe sipërmarrësi duhet të sigurojë se çdo raport auditimi nuk i ekspozon ato në mënyrë të paautorizuar.

Neni 11

Raportimi i incidenteve të sigurisë

1. Njoftimi fillestar i incidentit tek AKEP: Sipërmarrësit janë të detyruar të njoftojnë në rrugë elektronike, në AKEP, brenda 24 orëve nga evidentimi i incidentit me të dhënat e disponueshme në momentin e njoftimit. Ky njoftim është i detyrueshëm vetëm në rast se incidenti klasifikohet me impakt "mesatar" ose "të lartë". Ky njoftim duhet të përfshijë:
   a. Datën dhe orën e incidentit
   b. Shërbimin e prekur
   c. Natyrën e incidentit
   d. Impaktin paraprak të incidentit
   e. Kohëzgjatjen
2. Depozitimi i Aneksit 1 dhe Aneksit 2, brenda 72 orëve nga evidentimi i incidentit.
3. Njoftime të përditësuara, të Aneksit 1 dhe 2, në çdo moment, vetëm nëse ka një ndryshim të rëndësishëm në të dhënat e raportuara;
4. Raportimi përfundimtar i incidentit: Brenda 30 (tridhjetë) ditëve kalendarike nga evidentimi i incidentit të sigurisë, sipërmarrësit janë të detyruar të depozitojnë Aneksin 1 dhe Aneksin 2 me të dhënat e përditësuara.

5. Kur AKEP e vlerëson të arsyeshme për disa nga incidentet me impakt të lartë, sipërmarrësit duhet të dorëzojnë një raport i cili duhet të përfshijë, si më poshtë:
   a. Përmbledhje ekzekutive: çfarë ndodhi dhe kur, çfarë ndikimi pati (statistika finale), çfarë e shkaktoi dhe masat e marra;
   b. Shkaqet rrënjësore: analizë e detajuar e shkakut teknik/organizativ të incidentit (p.sh. "një gabim në konfigurimin e ruterve BGP lejojë një sulm route hijacking" ose "një punonjës dërgoi një email spear-phishing që instaloi malware");
   c. Masat korrigjuese dhe parandaluese: përshkrim i masave të marra për rimëkëmbjen (korrigjimin e problemit) dhe çfarë masa do të merren që një incident i ngjashëm të mos ndodhë në të ardhmen (p.sh. "do të implementojmë autentikim me dy faktorë për akses remote", "do të shtojmë monitorim 24/7 të trafikut", etj);
   d. Ndikimi i detajuar: numri i saktë i pajtimtarëve të prekur, kohëzgjatja totale e ndërprerjes së shërbimit, volumi i trafikut të humbur, dhe çdo pasojë tjetër (p.sh. dëme ekonomike të vlerësuara, dëmtim pajisjesh, etj).
   e. Komunikimet publike: nëse operatori ka informuar pajtimtarët ose publikun, të përshkruhet forma dhe koha kur është bërë (duke bashkëngjitur kopje të njoftimeve, nëse është e mundur);
   f. Bashkëpunimi institucional: të përmenden nëse janë përfshirë apo njoftuar institucione të tjera (p.sh. Policía e Shtetit për ndonjë aspekt kriminal, autoriteti përgjegjës për sigurinë kibernetike, Zyra e Komisionerit për mbrojtjen e të dhënave personale etj.).
6. **Mënyra e dorëzimit të njoftimeve:** Njoftimet sipas këtij neni dërgohen pranë AKEP, në rrugë elektronike në adresën zyrtare të dedikuar: incidente.raportimi@akep.al. Për dorëzimet sipas pikës 5 të këtij neni, njoftimi përveçse në rrugë elektronike, duhet të depozitohet edhe në rrugës zyrtare në AKEP.
7. **Informacion shtesë**: AKEP, mund të kërkojë në çdo kohë informacion shtesë mbi një incident të sigurisë, përtej të dhënave të përcaktuara në formular. Sipërmarrësit janë të detyruar t'i përgjigjen këtyre kërkesave pa vonesë, duke vënë në dispozicion të gjitha të dhënat përkatëse. Në këtë kuadër, operatorët duhet të ruajnë të gjitha të dhënat e lidhura me incidentin (log-e, evidenca hetimore, komunikimet e brendshme, etj.) për një periudhë jo më pak se 12 muaj nga data e dorëzimit të njoftimit përfundimtar. Kjo për të mundësuar që AKEP (ose autoritete të tjera të autorizuara) të kenë mundësi të kryejnë analiza të mëtejshme apo inspektime ex-post mbi incidentin.
8. **Incidentet që përfshijnë të dhëna personale:** Kur një incident teknik i sigurisë ka përfshirë edhe cenimin e të dhënave personale të përdoruesve/pajtimtarëve, sipërmarrësi detyrohet të kryejë njoftim të veçantë pranë Zyrës së Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, brenda 72 orëve nga zbulimi i cenimit të të dhënave. Ky njoftim do të përmbajë elementet e kërkuara në nenin 29 të ligjit "Për mbrojtjen e të dhënave personale". Në raportimin e tij tek AKEP, sipërmarrësi duhet të konfirmojë që ka kryer njoftimin tek Komisioneri (duke dhënë ref. të shkresës ose të emailit dërguar).
9. **Mungesa e përgjegjësisë shtesë nga njoftimi:** Akt i njoftimit të incidentit pranë autoriteteve, sipas detyrimeve të mësipërme, nuk e bën automatikisht sipërmarrësin përgjegjës ligjërisht për përmbajtjen ose pasojat e incidentit. Njoftimi konsiderohet

një veprim i mirëbesimit në kuadër të pajtueshmërisë dhe nuk do të përdoret për t'i ngarkuar sipërmarrësit përgjegjësi shtesë përtej atyre të parashikuara në ligj. Sidoqoftë, nëse hetimet e mëvonshme tregojnë shkelje të detyrimeve ose neglizhencë nga ana e sipërmarrësit, autoritetet kompetente mund të ndërmarrin masat ndëshkuese sipas legjislacionit në fuqi. Ky parashikim synon të inkurajojë raportimin e shpejtë dhe të plotë të incidenteve, pa frikën se vetë raportimi do të përdoret kundër raportuesit.

Neni 12

Kundërvajtjet administrative

Shkeljet e kësaj rregulloreje, kur nuk përbëjnë vepër penale, konsiderohen kundërvajtje administrative dhe dënohen me gjobë sipas parashikimeve të nenit 184 të ligjit nr. 54/2024 "Për komunikimet elektronike në Republikën e Shqipërisë".

Neni 13

Shfuqizime

Me hyrjen në fuqi të kësaj rregulloreje, Rregullorja nr. 37, datë 29.10.2015 "Mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike", shfuqizohet.

Neni 14

Hyrja në fuqi

Kjo Rregullore dhe Anekset që i bashkëlidhen, hyn në fuqi në datën e miratimit të saj nga Këshilli Drejtues i AKEP.

ANEKS 1 – Formulari i incidenteve të sigurisë

Seksioni	Fusha	Përmbajtja / Përshkrimi
I. Informacion kontakti	Të dhënat e sipërmarrësit	
	Emri dhe mbiemri i personit të ngarkuar me eliminimin e incidenteve të sigurisë dhe/ose cenimit të integritetit	
	Pozicioni i punës	
	Adresa	
	Telefon e-mail	
II. Përshkrimi i incidentit të sigurisë dhe/ose cenimit të integritetit	Lloji i incidentit	Përshkruaj natyrën e incidentit (p.sh. DDoS, ndërprerje infrastrukture, kompromet im sistemi, etj.)
	Data dhe ora e ndodhjes	
	Data dhe ora e zbulimit	
	Data dhe ora e rikuperimit	
	Shërbimi ose rrjeti i prekur	
	Zona gjeografike e ndikuar	
	Numri i përdoruesve të prekur	
	Kohëzgjatja e incidentit	
	Shkaku paraprak i incidentit	Përshkruaj shkakun e mundshëm (p.sh. gabim teknik, sulm, defekt, etj.)
	Ndikimi mbi rrjet dhe shërbimet	o I ulët o Mesatar o I lartë
	Masat e menjëhershme të marra	Veprimet e ndërmarra për rikuperim dhe minimizim impakti
	Masat parandaluese të planifikuara	
	Vlerësimi i impaktit	Plotësohet sipas Aneksit 2
III. Të dhëna shtesë	Evidenca teknike të bashkëngjitura	(log-e, raport auditimi, screenshot, etj.)
IV. Përfaqësuesi për kontakt	Emri, pozicioni, data dhe nënshkrimi	

ANEKS 2 – Vlerësimi i impaktit të incidentit te sigurisë

Një incident klasifikohet impakt të Lartë nëse ndodh të paktën një nga sa vijon:

1. **Preken shërbime kritike tw ofruara nga institucionet si më poshtë:**

    - Spitale dhe shërbime urgjence,
    - Institucione publike qe ofrojne sherbime kritike per publikun
    - Sektori Bankar
    - Infrastruktura si energjia dhe uji etj.

2. **Dështim i sistemit qendror / risk efekti domino:**

    - Dështim i backbone/core,
    - DNS/DHCP/AAA,
    - Interkoneksion/peering kryesor nderkombetar,
    - Defekt që rrezikon përhapje kombëtare.

Nëse nuk plotësohet asnjë nga kushtet e mësipërme, përdoret vlerësimi me pikë si në Tabelën 1 me poshte:

Kriteri		Ndikimi			
		I pandjeshem (=0)	I ulët (=1)	Mesatar (=2)	I lartë (=3)
1. Kohëzgjatja		30 min	30-120 min	2-6 h	> 6 h
2. Numri Përdoruesve	relativ %	<1%	1-5%	5-20%	> 20%
	absolut	<1,000	1,000-10,000	10,000-100,000	> 100,000
3. Shtrirja gjeografike		Nje site/node	Bashki/Qytet	Disa qarqe/rajone	Kombëtare
4. Shkalla e degradimit të Shërbimit		I lehtë	I dukshëm	I rëndë	Total
5. Ndikimi shoqëror/ekonomik		Pa ndikim	I kufizuar	I konsiderueshëm	Madhor

Tabela 1. Kriteret e Vlerësimit te Impaktit

Vlera për secilin Kriter në Tabelën 1, do jetë si më poshtë:

- I pandjeshëm = 0
- I ulët = 1
- Mesatar = 2
- I lartë = 3

Për kriterin e Numrit të Përdoruesve do merret vlera më e madhe midis kriterit relativ dhe atij absolut.

Përkufizimi i nivelit të ndikimit do bëhet sipas shumatores së të pestë kritereve:

- Impakt i Ulët 0–5 pikë
- Impakt i Mesëm 6–10 pikë
- Impakt i Lartë ≥11 pikë

ANEKS 3 – Masat e sigurisë kibernetike

Masat Organizative

Masat organizative të sigurisë kibernetike janë veprime administrative dhe procedurale, të ndërmarra nga operatorët e infrastrukturave kritike e të rëndësishme të informacionit, duke përfshirë, ndër të tjera, ndarjen e roleve dhe përgjegjësive për sigurinë, hartimin dhe miratimin e politikave dhe procedurave të sigurisë, menaxhimin e rrezikut kibernetik, ndërgjegjësimin dhe trajnimin e burimeve njerëzore, si dhe ndërtimin e një strukture organizative të dedikuar për sigurinë kibernetike.

Përmbushja e kërkesave të Aneksit A3, bëhet me vetëdeklarim formal nga ana e sipërmarrësve të komunikimeve elektronike, me kusht që sipërmarrësit të zotërojnë evidencë të plotë të brendshme si dhe dokumentacioni të jetë i disponueshëm për inspektim/auditim nga AKEP.

A1: Politika e sigurisë

Politika e sigurisë përfshin objektivat e sigurisë që lidhen me qeverisjen dhe menaxhimin e rreziqeve të sigurisë të rrjeteve të komunikimit dhe sistemeve të informacionit.

Masa e sigurisë	Implementimi
A. Vendosja e një politike të nivelit të larte, e miratuar nga stafi drejtues i infrastrukturës, që adreson sigurinë e rrjeteve të komunikimit dhe sistemeve kritike e të rëndësishme të informacionit dhe rishkimi periodik i saj. Rishikimi të bëhet minimumi njëherë në vit ose pas çdo incidenti të sigurisë kibernetike ose pas çdo ndryshimi madhor në infrastrukture.	A1. Politika e sigurisë se informacionit Dokument i miratuar nga stafi drejtues dhe përmban objektivat, fushën e zbatimit dhe parimet e sigurisë në rrjetet dhe sistemet e informacionit Versioni, data e miratimit etj. A2. Raportet e rishikimit periodik Evidencat që tregojnë data e rishikimit dhe detajet e ndryshimeve të bëra në politiken e sigurisë.

A2: Menaxhimi i rrezikut kibernetik

Të krijohet dhe të zbatohet një kuadër i përshtatshëm i menaxhimit të rrezikut për të identifikuar dhe për të trajtuar rreziqet për rrjetet e komunikimit dhe sistemet e informacionit.

Masa e sigurisë	Implementimi
A. Krijimi i një metodologjie për menaxhimin e rrezikut kibernetik. Rishikimi i saj të bëhet minimum njëherë në vit dhe/ose mbas çdo ndryshimi madhor në infrastrukturë.	A1. Dokument i metodologjisë së menaxhimit të rrezikut kibernetik duke përfshirë versionin, data dhe miratimin nga stafi menaxherial. A2. Raportet e rishikimit periodik dhe evidencat që tregojnë data e rishikimit dhe detajet e ndryshimeve të bëra në metodologjinë për menaxhimin e rrezikut.

B. Hartimi i një liste të rreziqeve për sigurinë e rrjeteve të komunikimit dhe sistemeve të informacionit, duke marre në konsiderate kërcënimet kryesore për asetet kritike. Rishikimi i saj të bëhet minimumi njëherë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukture.	B1. Lista e vlerësimit të rreziqeve të ardhura nga burime të ndryshme, duke përfshirë dhe rreziqet, të cilat vine nga palë të treta. B2. Njoftimi i stafit drejtues për listën e rreziqeve, si dhe vendimi i marrë për trajtimin e tyre. B3. Rishikimi i listës së rreziqeve dhe evidencat që tregojnë datat e rishikimit, detajet e ndryshimeve të bëra.
C. Hartimi i një plani për trajtimin e rreziqeve të identifikuara.	C1. Dokument i planit për trajtimin e rreziqeve. C2. Pasqyrimi i ndryshimeve të planit të trajtimit të rreziqeve.

A3: Siguria organizative

Të krijohet e të zbatohet një strukturë e përshtatshme e roleve të sigurisë dhe përgjegjësive për menaxhimin e sigurisë së informacionit.

Masa e sigurisë	Implementimi
A. Caktimi i roleve dhe përgjegjësive për menaxhimin e sigurisë së informacionit.	A1. Lista e roleve të sigurisë dhe përshkrimi i detajuar i përgjegjësive për secilin rol p.sh CISO, ISO, DPO, DBA, SYSADM etj. A2. Organigrama që tregon hierarkinë dhe lidhjet midis roleve të sigurisë. A3. Lista e kontakteve për personat përgjegjës për sigurinë e informacionit (emër, pozicion, kontakt)
B. Politika të qarta për transparencën e përdorimit dhe afatet e ruajtjes së të dhënave personale të log-eve dhe metadatave	B1. "Sipërmarrësi siguron që përdoruesit dhe pajtimtarët informohen në mënyrë të qartë, të kuptueshme dhe të aksesueshme për sa mund të konsiderohet përpunimin i të dhënave personale në kuadër të masave të sigurisë së rrjeteve (log-e, monitorim trafiku, sisteme etj.) B2. "Sipërmarrësi përcakton dhe dokumenton afatet e ruajtjes së të dhënave personale për proceset përpunuese që zhvillon në zbatim të kësaj rregullore.

A4: Kërkesat e sigurisë kibernetike për palët e treta

Të krijohet e të zbatohet një politikë me kërkesa sigurie për kontratat me palët e treta për të siguruar që marrëdhëniet me palët e treta të mos ndikojnë negativisht në sigurinë e rrjeteve të komunikimit e të sistemeve të informacionit.

Çdo delegim i përpunimit të të dhënave personale tek palët e treta bëhet mbi bazën e një kontrate të posaçme, në përputhje me legjislacionin në fuqi për mbrojten e të dhënave personale, ku të përcaktohen objektivi, natyra dhe qëllimi i përpunimit, lloji i të dhënave, kategoritë e subjekteve, masat teknike dhe organizative të sigurisë, si dhe detyrimet dhe përgjegjësitë e palës së tretë ndaj sipërmarrësit.

Masa e sigurisë	Dokumentim / Verifikim i implementimit
A. Vendosja e një politike sigurie për furnizimet/ kontratat me palë të treta dhe rishikimi në mënyrë periodike i saj. Minimum njëherë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturë.	A1. Politika e sigurisë për furnizimet/ kontratat me palët e treta (version, data e publikimit, miratimi). A2. Raporte të rishikimit periodik të politikes së sigurisë dhe ndryshimet e realizuara.
B. Përfshirja e kërkesave të sigurisë në kontratat me palët e treta, duke përfshirë konfidencialitetn dhe transferimin e sigurt të informacionin.	B1. Kërkesa të qarta sigurie ne kontratat me palët e treta. B2. Marrëveshje konfidencialiteti për ruajtjen e informacionit me palet e treta.
C. Mbajtja e gjurmëve/ rekordeve të incidenteve të sigurisë kibernetike, që lidhen ose janë të shkaktuara nga palët e treta	C1. Regjistri i incidenteve kibernetike të lidhura me palët e treta (data,shkaku, ndikimi, veprimet)

A5: Siguria e burimeve njerëzore dhe aksesit të personave

Të vendoset e të zbatohet një politikë për sigurinë dhe mbrojtjen e të dhënave personale për ndërgjegjësimin e burimeve njerëzore, si dhe të aksesit të personave, në bazë të objektivave të sigurisë në lidhje me personelin.

Masa e sigurisë	Implementimi
A. Vendosja e një politike për sigurinë dhe për mbrojtjen e të dhënave personale për burimet njerëzore.	A1. Politika e sigurisë dhe e mbrojtjes së të dhënave personale, për burimet njerëzore (përfshirë të gjitha fazat: para rekrutimit, gjate punësimit, proceset disiplinore, në përfundim të marrëdhënies së punësimit). A2. Dokumenti i verifikimit të integritetit të personelit kryesor (vërtetim të gjendjes gjyqësore, referenca të punëve të mëparshme, certifikime, CV etj.) A3. Procedura për mbrojtjen e të dhënave personale.
B. Implentimi i një program trajnimi për sigurinë kibernetike dhe për mbrojtjen e të dhënave personale (Rishikim minimum njëherë në vit)	B1. Program i detajuar i trajnimit, i përshtatur sipas roleve dhe përgjegjësive të punonjësve. B2. Lista e pjesëmarrësve dhe datat e trajnimeve B3. Dokumenti i realizimit të fushatave të ndërgjegjësimit/ trajnimit të punonjësve në lidhje me sigurinë kibernetike dhe me sulmet më të shpeshta si “Phishing”, “Malëare” dhe për mbrojtjen e të dhënave personale, etj.
C. Informimi dhe trajnimi i punonjësve të rinj për politikat dhe procedurat në fuqi për sigurinë kibernetike	C1. Evidenca për trajnim për punonjësit e rinj. C2. Formularë të nënshkruar nga punonjësit për njohjen e politikave dhe procedurave. C3. Formularë të nënshkruar nga punonjësit për marrëveshjen e konfidencialitet (“NDA – Non Disclosure Agreement”).

A6: Menaxhimi i aseteve

Të krijohen e të zbatohen procedurat e menaxhimit të aseteve dhe kontrollet e konfigurimit për të siguruar disponueshmërinë e aseteve kritike dhe konfigurimet e rrjeteve të komunikimit e të sistemeve të informacionit.

Masa e sigurisë	Implementimi
A. Marrja e masave për identifikimin dhe menaxhimin efektiv të aseteve. (Minimumi 1 (një) herë në vit dhe/ose apo pas çdo ndryshimi madhor në infrastrukturën	A1. Inventari i plote i aseteve të teknologjisë së informacionit duke përfshirë kategorinë e aseteve, nr. serie, protokolli i internetit, vendndodhjen, vjetërsinë, statusin e tyre. A2. Vendosja në inventor i ndikimit, sipas konfidencialitetit, integritetit dhe disponueshmërisë.
B. Vendosja dhe zbatimi i politikave/ procedurave për menaxhimin e aseteve.	A1. Politika/procedura të detajuara për menaxhimin e aseteve, duke përfshirë rolet dhe përgjegjësitë, asetet që janë objekt i kësaj politike/procedure, objektivat e menaxhimit të aseteve, si dhe shkatërrimin e aseteve. (Rishikim minimumi 1 (një) herë në vit dhe/ose pas çdo ndryshimi madhor në infrastructure) A2. Topologji e detajuar e rrjetit dhe sistemeve të informacionit
C. Marrja e masave për zëvendësimin ose izolimin e sistemeve që iu ka përfunduar cikli i jetës (“EOL”- End of Life).	C1. Dokument ose evidencë të identifikimit të sistemeve që iu ka përfunduar cikli i jetës (EOL) dhe planifikimi për zëvendësimin/izolimin e tyre. C2. Evidenca të zëvendësimit/izolimit të asetit, i cili ka arritur kohën e ciklit të jetës (EOL). C3. Verifikimi i sistemeve dhe evidencat.
D. Kryerja e azhurnimeve (“patch-imeve”) automatike/manuale në sistemet fundore dhe në të gjithë infrastrukturën e teknologjisë së informacionit (IT) dhe teknologjisë operacionale (OT).	D1. Procedurë për menaxhimin e zbatimit të azhurnimeve (patch-eve) për pajisjet dhe sistemet e teknologjisë së informacionit (IT) dhe teknologjisë operacionale (OT), përfshirë frekuencën, përgjegjësit, rekorde. D2. Verifikimi i sistemeve/ mjeteve (“tools”) dhe evidencat.
E. Përcaktimi dhe zbatimi i politikave e i kontrolleve të sigurisë për pajisjet personale të përdorura për akses në sistemet dhe të dhënat e infrastrukturës (“BYOD” – Bring Your Oën Device”), duke siguruar mbrojtjen e informacionit dhe pajtueshmërinë me standardet e sigurisë.	E1. Politikë/procedurë për përdorimin e pajisjeve personale (telefona, laptop, tableta etj.), si dhe një inventar të pajisjeve personale të autorizuara për t’u përdorur në rrjetet dhe sistemet e brendshme të infrastrukturës E2. Evidenca te konfigurimeve minimale të sigurisë së pajisjeve personale sipas politikës.

A7: Menaxhimi i incidenteve të sigurise kibernetike

Të hartohen e të zbatohen plane e procedura për menaxhimin e incidenteve kibernetike, duke përfshirë zbulimin, reagimin, raportimin dhe komunikimin e tyre.

Masa e sigurise	Implementimi
A. Hartimi i planeve dhe procedurave të detajuara për menaxhimin e incidenteve të sigurisë kibernetike. (Rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturë)	A1. Dokumenti i planit për menaxhimin e incidenteve kibernetike (versioni, data, miratimi). A2. Procedura për identifikimin, klasifikimin dhe trajtimin e incidenteve (manual veprimi - "Playbooks"), lista e personave të ekipit për reagimin ndaj incidenteve kibernetike.
B. Ruajtja e të dhënave për të gjitha incidentet e sigurisë kibernetike.	B1. Regjistri i incidenteve që përfshin: datën, shkakun, ndikimin dhe veprimet korrigjuese. B2. Raporte individuale të trajnimit të incidenteve dhe analizat e mësimeve të nxjerra.
C. Përcaktimi dhe zbatimi i komunikimeve dhe raportimeve të incidenteve kibernetike me autoritetet dhe njoftimi i paleve të treta dhe klientëve.	C1. Formularë raportimi të incidenteve për autoritetet e përcaktuara në legjislacion në fuqi për sigurinë kibernetike nga ana e infrastrukturës. C2. Inventari i komunikimeve dhe raportimeve.

A8: Menaxhimi i ndryshimeve

Të përcaktohen e të zbatohen politikat dhe proceset për menaxhimin e ndryshimeve përmes planifikimit, vlerësimit, miratimit, komunikimit, implementimit dhe monitorimit të ndryshimeve në infrastrukturë.

Masa e sigurisë	Implementimi
A. Sigurimi se çdo ndryshim në sistemet dhe proceset e infrastrukturës së teknologjisë së informacionit (IT) brenda infrastrukturës kritike/të rëndësishme, menaxhohet në mënyrë të kontrolluar dhe të dokumentuar.	A1. Politika e menaxhimit të ndryshimeve (përfshirë përshkrimin, datën, përgjegjësitë dhe impaktin e parashikuar, planin e zbatimit etj.). (Rishikim minimumi 1 (një) herë në vit.) A2. Procedura e menaxhimit të ndryshimeve (hapat nga propozimi deri tek miratimi dhe implementimi) A3. Formulari i kërkesës për ndryshim ("RFC" – Request for Change)

A9: Menaxhimi i vazhdimësisë së punës

Të krijohen e të zbatohen plane emergjence dhe një strategji e qartë për të siguruar vazhdimësinë e rrjeteve të komunikimit e të sistemeve të informacionit

Masa e sigurisë	Dokumentim / Verifikim i implementimit

A. Krijimi dhe zbatimi i një plani të vazhdimësisë së biznesit ("BCP"- Business Continuity Plan) për të siguruar funksionimin e vazhdueshëm të proceseve kritike të infrastrukturës në rast të incidenteve kibernetike, fatkeqësive natyrore ose ndërprerjeve operacionale. (Rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturë.	A1. .Politika e strategjisë për vazhdimësinë e shërbimeve, duke përfshirë kushtet për aktivizimin e planit, kohën e rikuperimit, komunikimin në kohë krize, skenarët e incidenteve, planin e veprimit, rregullat e testimit etj. A2. Analiza e ndikimit në biznes ("BIA" - Business Impact Analysis), identifikimi i proceseve kritike dhe përcaktimi i objektivit të kohës/pikës së rikuperimit ("RTO" – Recovery Time Objective / "RPO" – Recovery Time Objective). A3. Lista e kontakteve emergjente – informacion për pikat e kontaktit në rast krize.
B. Realizimi i një politike/procedure për kryerjen e kopjeve rezervë (backup). (Rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturë.	B1. Dokumenti i politikës/procedurës për kryerjen e kopjeve rezervë (backup-it), duke përfshirë frekuencat, llojet, të dhënat dhe shërbimet. B2. Lista e kopjeve rezervë (backup-eve) të kryera dhe raportet e testimit të rikuperimit dhe integritetit të të dhënave.
C. Shmangia e pikave të vetme të dështimit (Single Point of Failure) në shërbimet kritike dhe të rëndësishme të infrastrukturës	C1. Verifikimi teknik i pikave të vetme të dështimit. C2. Evidenca për redundancën e shërbimeve
D. Implementimi i infrastruktures sipas skemave te sherbimit ne vazhueshmeri te larte (HA – High Availability)	D1. Dokument i skemave të infrastrukturës sipas shërbimit me disponueshmëri të lartë (HA) ne nivelet e mbeshtetjes teknike te livelit te pare, te dyte dhe te trete(L1, L2, L3) dhe perimetrit me fireëall.
E. Implementimi i një ambienti të dytë për rikuperimin dhe vazhdueshmërinë e funksionimit të sistemeve të teknologjisë së informacionit (IT) pas një incidenti kibernetik ("DRS" – Vendi i rikuperimit nga katastrofa/Disaster Recovery Site).	E1. Strategjia për DRS-në dhe konfigurimet e detajuara. (Rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së). E2. Plani i rikuperimit nga fatkeqësitë (DRS), procedurat për rikuperimin e teknologjisë së informacionit (IT) dhe infrastrukturës (detyrat dhe përgjegjësitë, lista e sistemeve dhe aseteve kyçe), (rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor ne infrastrukture. E3. Raporte të testimit të ambientit të dytë për rikuperimin dhe vazhdueshmërinë e funksionimit të sistemeve të teknologjisë së informacionit për rikuperim pas incidenteve/katastrofave (DRS). (Minimumi 1 herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhore në infrastrukturë. E4. Verifikim dhe evidence.

A10: Menaxhimi i pajtueshmërisë ligjore

Të krijohen e të zbatohet një politikë për monitorimin e pajtueshmërisë së standardeve me kërkesat ligjore.

Masa e sigurisë	Implementimi
A. Monitorimi i pajtueshmërisë së standardeve me kërkesat ligjore.	A1. Politikë/procedurë për monitorimin e pajtueshmërisë me standardet dhe kërkesat ligjore. A2. Lista e standardeve dhe kërkesave ligjore të aplikueshme për infrastrukturën. A3. Rishikimi i politikave dhe procedurave për sistemin e menaxhimit të informacionit ("ISMS" – Information Security Management System), minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturë.

Sipërmarrësi miraton dhe zbaton procedura të dokumentuara për pranimin dhe trajtimin e kërkesave për akses, korrigjim, fshirje, kufizim, kundërshtim për përpunimin e të dhënave personale, si dhe koordinimin ndërmjet nëpunësit për mbrojtjen e të dhënave personale dhe strukturës së sigurisë së rrjeteve për çdo rast që lidhet me të drejtat e subjekteve të të dhënave.

A11: Kontrolli dhe auditimi

brendshme e të jashtme, me qëllim monitorimin e pajtueshmërisë dhe përmirësimin e vazhdueshëm të sigurisë së informacionit në infrastrukturë.

Masa e sigurise	Implementimi
A. Politikë/procedurë për kontrollin dhe auditimin e brendshëm për sigurinë e informacionit dhe rishikimi në mënyrë periodike. (Minimumi 1 herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturë).	A1. Dokument i politikës/ procedurës për kontrolle dhe auditime (versioni, data, miratimi i politikës/procedurës nga stafi menaxherial).
B. Kryerja e kontrolleve/auditeve të brendshme ose nga palët e treta për sigurinë e informacionit dhe sistemeve kritike të infrastrukturës. (Minimumi 1(një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturë).	B1. Raporte të auditimeve të brendshme dhe plani i trajtimit të mangësive(data, metodologjia, rezultatet). B2. Raporte të auditimeve të realizuara nga palët e treta për sigurinë e informacionit. B3. Lista e veprimeve korrigjuese të ndërmarra pas auditimeve dhe evidenca e implementimit të tyre.

B. Masat teknike dhe operacionale

Masat teknike të sigurisë kibernetike janë zgjidhje dhe mekanizma teknologjikë, që garantojnë mbrojtjen dhe integritetin e rrjeteve të komunikimit dhe sistemeve të informacionit të operatorëve të infrastrukturave të informacionit, duke përfshirë zbatimin e kontrollit të aksesit, autentifikimin

dhe autorizimin, enkriptimin e të dhënave, monitorimin dhe regjistrimin e ngjarjeve të sigurisë, mbrojtjen nga sulmet kibernetike, si dhe zbatimin e teknologjive për zbulimin dhe parandalimin e incidenteve të sigurisë kibernetike. Ndërsa, masat operacionale të sigurisë kibernetike janë proceset, praktikat dhe aktivitetet e përditshme të operatorëve të infrastrukturave të informacionit për garantimin e sigurisë së informacionit dhe funksionimin e qëndrueshëm të sistemeve kritike e të rëndësishme, duke përfshirë menaxhimin e incidenteve të sigurisë kibernetike, sigurimin e vazhdimësisë së shërbimeve dhe rikuperimin nga katastrofat, menaxhimin e ndryshimeve në infrastrukturë, si dhe aplikimin e procedurave për raportim dhe komunikim të ngjarjeve të sigurisë me autoritetet përgjegjëse

B1: Siguria fizike

Të krijohet e të zbatohet siguria e duhur fizike dhe mjedisore e rrjeteve/ sistemeve te informacionit e pajisjeve.

Masa e sigurise	Dokumentim / Verifikim i implementimit
A. Implementimi i masave të sigurisë fizike dhe kontrolleve mjedisore.	A1. Evidenca të implementimit të masave të sigurise fizike (brava, kabinete, kontroll elektronik i hyrjes). A2. Gjurmë të aktiviteteve (logs) të auditimit për aksesin në hapësira të autorizuara dhe alarme për hyrjet e paautorizuara. A3. Raporte të funksionimit dhe mirëmbajtjes së sistemeve të alarmit dhe fikësve të zjarrit. A4. Të sigurohet ndarja e hapësirave fizike në zona të segmentuara bazuar në nivelet e autorizimit, duke përfshirë hartimin e një topologjie të detajuar dhe një plani të qartë evakuimi për të garantuar sigurinë fizike dhe menaxhimin e aksesit.
B. Implementimi i një politike për masat e sigurisë fizike dhe kontrollet mjedisore.	B1. Dokumenti i politikës për sigurinë fizike dhe kontrollet mjedisore (versioni, data, miratimi, rishikimi).

B2: Menaxhimi për autorizimin e aksesit

Të krijohen e të mirëmbahen kontrollet e autorizimet e duhura të aksesit në rrjetet e komunikimit dhe sistemet e informacionit.

Masa e sigurise	Implementimi
A. Implementimi i politikave për kontrollin dhe mbrojtjen e aksesit në rrjetet dhe sistemet e informacionit. (Rishikim minimumi 1 (një) herë në vit dhe/ose pas çdo ndryshimi madhor në infrastrukturën	A1. Dokument i politikës për aksesin (role, grupe, të drejta, procedurat e dhënies dhe revokimit të aksesit). A2. Formular për dhënie të drejtash aksesi A3. Formular për revokim të drejtash aksesi dhe dorëzimi asetesh. A4. Evidenca për fshirjen e llogarive gjenerike dhe raportet e kontrolleve periodike te aksesit.
B. Aplikimi i filtrave për trafikun në rastin e aksesimit në distancë të	B1. Verifikimi teknik dhe evidencat për vendosjen e filtrave dhe enkriptimin e trafikut.

sistemeve, si dhe enkriptimi i trafikut me protokolle të sigurta	
C. Kontrolli nëse në fireëall ka të konfiguruar lista të autorizuara/lista të bllokuara (“Ëhitelist/Blacklist”) të adresave të protokollit të internetit (IP) të lejuara ose bllokuara	C1. Verifikim dhe evidenca për konfigurimet në murin mbrojtës digjital (fireëall).
D. Perdorimi i politikave për menaxhimin e fjalëkalimeve rastësore për perdoruesit dhe administratorët lokale.	D1. Dokumenti i politikës për menaxhimin e fjalëkalimeve dhe verifikim i implementimit të zgjidhjeve për menaxhimin e fjalëkalimeve rastësore për përdoruesit dhe administratorët lokalë (“LAPS”- Local Administrator Passëord Solution) ose teknologji të ngjashme.
E. Krijimi dhe implementimi i një zgjidhje teknologjike për menaxhimin e identiteteve dhe aksesit të përdoruesve (“IAM” – Identity and Access Management) për të garantuar sigurinë, autorizimin dhe auditimin e aktiviteteve të përdoruesve në sistemet kritike.	E1. Verifikim teknik dhe evidenca.
F. Implementimine e një zgjidhjeje teknologjike për menaxhimin e akseseve të privilegjuara(“PAM”- Priviledged Access Management)	F1. Verifikim teknik dhe evidenca.
G. Implementimi i shërbimit të sigurisë me akses në rrjet, sipas parimit me zero besim (“ZTNA” – Zero Trust Netëork)	G1. Verifikim teknik dhe evidenca.

B3: Pajisjet kriptografike

Të sigurohet përdorimi i mjaftueshëm i enkriptimit për të parandaluar dhe/ose për të minimizuar ndikimin e incidenteve të sigurisë kibernetike të përdoruesit në rrjetet e komunikimit dhe në sistemet e informacionit.

Masa e sigurisë	Implementimi
A. Implementimi i politikave të enkriptimit, duke përfshirë detaje rreth algoritmeve dhe çelësave kriptografikë.	A1. Dokumenti i politikës së enkriptimit si p.sh. algoritmet: “AES”, “RSA”, “ECC”, “TLS”, “IPSec”, “SSH” etj. A2. Lista e çelësave kriptografikë (p.sh., lloji, afati i vlefshmërisë, metoda e gjenerimit dhe ruajtjes).
B. Kriptimi i të dhënave (në transit dhe në gjendje të qëndrueshme)	B1. Lista e konfigurimeve të kriptimit për të dhënat dhe aplikacionet (“on-prem”, “hybrid”, “cloud”). B3. Verifikimi teknik dhe evidenca

B4: Zbulimi i incidenteve të sigurise kibernetike

Të krijohen e të mirëmbahen kapacitete për zbulimin e incidenteve të sigurisë kibernetike.

Masa e sigurisë	Implementimi
A. Implementimi i sistemit të automatizuar për zbulimin dhe menaxhimin e informacionit e të incidenteve/ngjarjeve të sigurisë ("SIEM" - Security Information and Event Management).	A1. Verifikim teknik dhe evidenca të konfigurimit të sistemit të automatizuar për zbulimin dhe menaxhimin e informacionit e të incidenteve/ngjarjeve të sigurisë (SIEM), përfshirë rregullat e alarmimit e të filtrimit të gjurmëve dhe aktiviteteve (log-eve) për zbulimin e incidenteve.

B5: Mbledhja dhe përpunimi i informacionit për kërcënimet kibernetike

Të krijohet e të mirëmbahet një mekanizëm për monitorimin, mbledhjen dhe analizën e informacionit në lidhje me kërcënimet e sigurisë në rrjetet e komunikimit dhe në sistemet e informacionit.

Masa e sigurisë	Implementimi
A. Monitorimi i vazhdueshëm i burimeve të jashtme të inteligjencës për kërcënimet kibernetike "threat intelligence".	A1. Raporte periodike nga mjetet e monitorimit të inteligjencës për kërcënimet kibernetike "threat intelligence". A2. Lista e burimeve të përdorura për mbledhjen e informacionit për kërcënimet
B. Zbatimi i programit të inteligjencës për kërcënimet kibernetike "threat intelligence", në të cilin të përfshihen rolet, përgjegjësitë dhe procedurat.	B1. Dokument i programit të inteligjencës për kërcënimet kibernetike "threat intelligence" (përfshirë strukturën e roleve dhe përgjegjësive). B2. Procedura për mbledhjen, përpunimin, analizën dhe shpërndarjen e informacionit për kërcënimet kibernetike.

B6: Monitorimi dhe regjistrimi i ngjarjeve të sigurisë kibernetike

Të krijohen e të mirëmbahen sisteme dhe funksione për monitorimin dhe regjistrimin e ngjarjeve të sigurisë në rrjetet kritike e në sistemet e informacionit.

Masa e sigurisë	Implementimi
A. Implementimi i politikave për monitorimin dhe regjistrimin e ngjarjeve të sigurisë kibernetike	A1. Dokument i politikave për monitorimin dhe regjistrimin e gjurmëve e të aktiviteteve (log-eve), ku përfshihen kërkesat minimale, periudha e mbajtjes, objektivat, miratimi, përditësimi.
B. Vendosja e mjeteve për mbledhjen e gjurmëve dhe aktiviteteve (log-eve) të sistemeve kritike.	B1. Lista e mjeteve të implementuara për mbledhjen e gjurmëve dhe aktiviteteve/ logeve të log servers etj. B2.Verifikim teknik dhe evidenca.

B7: Mbrojtja e integritetit të rrjeteve të komunikimit

Të krijohet dhe të ruhet integriteti i rrjeteve dhe sistemeve të informacionit, si dhe të mbrohen nga viruset, injeksionet e kodeve dhe malëare-ve të tjerë, që mund të ndryshojë funksionalitetin e sistemeve.

Masa e sigurisë	Implementimi
A. Instalimi i pajisjeve për të monitoruar për të kontrolluar dhe për të kufizuar trafikun hyrës e dalës të rrjeteve kompjuterike me murin mbrojtës digjital të gjeneratës së re (“Next Generation Fireëall”)	A1. Verifikim teknik për konfigurimin të murit mbrojtës digjital i gjeneratës së re. A2. Verifikim teknik dhe evidencat.
B. Monitorimi, zbulimi dhe analiza e sjelljeve të dyshimta sjellje (behaviour) në pajisjet fundore (endpoints), si kompjuterët, laptopët dhe serverët. Ky sistem mbledh dhe analizon të dhëna nga pajisjet fundore për të zbuluar kërcënime të sofistikuara.	B1. Verifikim teknik dhe evidenca të analizave të trafikut.
C. Ndarja e rrjetit në nënrrjete në nivel mikrosegmentimi	C1. Verikimi teknik dhe evidenca e topologjisë së rrjetit me ndarjen e dokumentuar në nënrrjete.
D. Vendosja në zona/ nënndarje të rrjetit/ rrjet lokal virtual(zone/ subnet/ VLAN – Virtual Local Area Netëork) të ndryshme të kompjuterave dhe serverave me list atë aksesit të kontrollit (Access Control List) sipas parimit të të drejtave minimale (“last privilege”)	D1. Lista e rrjeteve local virtual (VLAN) dhe nënndarje të rrjetit të implementuara, përfshire listat e kontrollit të aksesit. D2. Verifikim teknik dhe evidencat.
E. Izolimi i rrjetit ëireless nga pjesa tjetër e rrjetit.	E1. Verifikim teknik dhe evidencat e konfigurimit të izolimit të rrjetit ëireless
F. Përdorimi i teknikave të sigurisë së portave të sëitch-it (“sëitch port security”) “për të kufizuar numrin e adresave unike të identifikimit të pajisjes së lidhur në rrjet (MAC Address) në “1” për përdoruesit e thjeshtë dhe në një numër të kufizuar për ekspertët e teknologjisë të informacionit ose sigurisë kibernetike.	F1. Verifikimi teknik i konfigurimit të sëitch-eve, duke zbatuar teknikën e sigurisë së portave “Port Security” për numrin unik të identifikimit të pajisjes së lidhur në rrjet (MAC Address) të lejuara.
G. Zbatimi i teknikave dhe standardeve për fortifikimin(“hardening”) e të gjitha pajisjeve në rrjet.	G1. Manual për fortifikimin e pajisjeve (PC, server, router, fireëall). G2. Verifikim teknik dhe evidencat.
H. Izolimi logjikisht i bazës së të dhënave dhe shërbimet ËEB(p.sh. në rrjet local virtual/VLAN të ndryshëm).	H1.Lista e rrjetit local virtual VLAN dhe verifikimi teknik i konfigurimit për izolimin logjik të bazës së të dhënave dhe shërbimeve ËEB.
I. Implementimi i “DNS_SEC” për të shmangur “DNS Amplification” dhe “DNS Poisonning”.	I1. Verifikim teknik dhe evidencat.
J. Zbatimi i mbrojtjes ndaj sulmeve DoS/DDoS	J1. Verifikim teknk i konfigurimit të mekanizmave të mbrojtjes nga DoS/DDoS(p.sh. “rate limiting”,”ËAF” – Ëeb Application FireËall, mjete(tools) per “anti-DDoS”)
K. Implementimi i një zgjidhjeje/sisteme për kontrollin e parametrave të sigurise së pajisjeve	K1. Procedure për përcaktimin e parametrave të sigurisë minimale(baseline). K2. Verifikim teknik dhe evidencat.

fundore(“NAC“- Netëork Access Control)	

B8: Menaxhimi i aksesit të përdoruesve

Të implementohen politikat për menaxhimin e fjalëkalimeve dhe dhënien e aksesit sipas modeleve kontroll diskrecional i aksesit(“DAC” – Dicretionary Access Control), kontroll i detyrueshem i aksesit(“MAC”- Mandatory Access Control) dhe kontroll i aksesit bazuar në role(RBAC – Role Based Access Control). Të përdoret shërbimi Active Directory (AD) për menaxhimin e privilegjeve dhe kufizimin e aksesit të paautorizuar në pajisje.

Masa e sigurise	Implementimi
A. Implementimi i politikave për menaxhimin e fjalëkalimeve të përdoruesve	A1. Dokument i politikës për menaxhimin e fjalëkalimeve (kompleksiteti, afati i skadimit, ndryshimet periodike).
B. Modelet për dhënien e aksesit të përdoruesve (kontroll diskrecional i aksesit (DAC), kontroll i detyrueshëm i aksesit (MAC) dhe kontroll i aksesit bazuar në role (RBAC)	B1. Evidenca teknike të konfigurimeve e të rregullave të zbatuara në sistem dhe verifikim.
C. Menaxhimi i aksesit dhe privilegjeve të përdoruesve përmes shërbimit “AD”	C1. Verifikim teknik dhe evidenca të implementimit të “AD”-në (strukturat e grupeve, privilegjet, kufizimet)
D. Sigurimi dhe mbrojtja e të dhënave dhe kufizimi i aksesit të paautorizuar dhe informacion.	D1. Verifikim i zbatimit të politikës / procedurës “Clean Desk” dhe politikës / procedures se kycjes automatike të ekranit pas një kohe passive (“idle”)
E. Implementimi i sistemeve me dy faktore autentifikimi (2FA – Tëo- Factor Authentication) në nivel aplikacioni /ëeb/mail/ pajisje për të gjithë përdoruesit e sistemit kritik	E1. Verifikimi dhe evidenca.

B9: Veprimtaria dhe autentifikimi i administratorëve

Të sigurohet aksesi i administratorëve, duke zbatuar autentifikimin me shumë faktorë (“MFA”- Multi-Factor Authentication) në aplikacione, ëeb, email dhe pajisje. Të përdoren platforma për parandalimin e humbjes së të dhënave (“DLP” - Data Loss Prevention) për parandalimin e rrjedhjes së paautorizuar të informacionit.

Masa e sigurisë	Implementimi
A. Implementimi i metodës së autentifikimit me shumë faktorë (MFA), në nivel aplikacion/ëeb/ mail/ pajisje për administratorët	A1. Verifikimi dhe evidencat e implementimit te metodës së autentifikimit me shumë faktorë (MFA).
B. Përdorimi i metodës për parandalimin e humbjes së të dhënave (DLP) për identifikimin dhe parandalimin e rrjedhjes së paautorizuar	B1.Verifikimi i implementimit të metodës për parandalimin e humbjes së të dhënave (DLP) për rrjedhjen e të dhënave të ndjeshme.

të të dhënave të ndjeshme jashtë infrastrukturës.	

B10: Siguria e aplikacioneve

Të sigurohet mbrojtja e aplikacioneve, duke kryer testime të sigurisë për vlerësimin e dobësive ("VA" – Vulnerability Assessment) dhe testimi i penetrimit ("Penetration Test") e duke trajtuar problematika e evidentuara.

Masa e sigurisë	Implementimi
A. Kryerja e testimeve për vlerësimin e sigurisë së aplikacioneve e rrjeteve të teknologjisë së informacionit për vlerësimin e dobësive (VA) dhe hartimi i planit për trajtimin e problematikave të evidentuara. (Minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukure.	A1. Raporti i vlerësimit të dobësive dhe plani i trajtimit.
B. Kontrolli nëse shërbimet ëeb ("ëeb services") operojnë duke zbatuar protokollin e sigurt "https".	B1. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "screenshot", log-eve dhe dokumentimit të detajuar të parametrave teknikë).
C. Konfigurimi i "anti-spoofing": DMARC /SPF/DKIM në sistemin e e-mail-it.	C1. Verifikimi teknik dhe evidencat (p.sh. evidenca e implementimit të anti-spoofing në sistemin e e-mail-it)
D. Realizimi i testimeve të zhvillimit të softëare-ve ("staging/testing") në ambient të dedikuar dhe të ndarë nga ambienti i prodhimit ("production"), nëse infrastruktura ka një departament zhvillimi.	D1. Verifikimi i evidencave të ambientit të dedikuar për testime të softëare-ve, të ndarë nga ambienti i prodhimit.
E. Implementimi i një zgjidhjeje për filtrimin, monitorimin dhe bllokimin e trafikut keqdashës në internet, me fireëall për sigurinë e aplikacioneve ËEB (ËAF – Ëeb Application Fireëall)	E1. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes screenshot, log-eve dhe dokumentimit të detajuar të parametrave teknikë).
F. Implementimi i "Reverse Proxy" në një server që qëndron midis klientëve dhe serverëve të brendshëm "backend servers" dhe vepron si ndërmjetës për të përpunuar kërkesat nga klientët dhe për t'i përcjellë ato te serverët e brendshëm.	F1. Verifikimi i implementimit të "Reverse Proxy" në serverat ëeb (p.sh. evidenca vizuale të konfigurimeve përmes screenshot, log-eve dhe dokumentimit të detajuar të parametrave teknikë).
G. Kryerja e testimeve për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (Penetration Test – Black, Gray, Ëhite) dhe hartimi i një plani për trajtimin e problematikave të evidentuara.	G1. Raporti i testimeve të llojeve: "black", "grey", "ëhite" për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (penetration test) dhe plani i trajtimit.

(Minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën	

B11: Siguria e prodhimit të softëare-ve

Siguria e prodhimit të softëare-ve për infrastrukturat kritike apo të rëndësishme përfshin praktikat dhe masat që mundësojnë projektimin, zhvillimin, testimin, dhe implementimin e softëare-ve me siguri të lartë për të mbrojtur infrastrukturat nga sulmet kibernetike.

Masa e sigurisë	Implementimi
A. Implementimi i një procedure sigurie për projektimin dhe zhvillimin e softëare-ve. (Rishikim njëher në vit.)	A1. Dokumentim i procedurës së sigurisë për projektimin dhe/ose zhvillimin e softëare-ve. A2. Procedura duhet të miratohet nga stafi i lartë menaxherial dhe të rishikohet në mënyrë periodike.
B. Kontrolli dhe monitorimi i aksesit të zhvilluesve dhe përdoruesve të softëare-ve.	B1. Të përfshihen në procedurë specifika, si mënyra e autentifikimit, autorizimit, enkriptimit për zhvilluesit e softëare-ve. B2. Të përcaktohen qartë të drejtat dhe akseset për përdoruesit e softëare-ve
C. Ruajtja e historikut të ndryshimeve/ konfigurimeve/ aprovimit të zhvillimit të kodit burim (source code) të softëare-it.	C1. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes “screenshot”, log-eve dhe dokumentimit të detajuar të parametrave teknikë).
D. Analiza e rrezikut dhe sigurisë të softëare-it para se të dalë në prodhim (production).	D1. Raporte të analizës së rrezikut dhe sigurisë së softëare-it para se të dalë në prodhim, duke përfshirë dhe varësinë nga libraritë e palëve të treta.
E. Trajtimi dhe dokumentimi i incidenteve të sigurisë kibernetike për zhvillimin e softëare-ve	E1. Raportet e auditit dhe log-et e incidenteve të zhvillimit të softëare-ve.
F. Monitorimi i vendit të ruajtjes(repository) së kodit burim të softëare-it.	F1. Raporte monitorimi të vendit të ruajtjes (repository) së kodit burim të softëare-it
G. Realizimi i lidhjes së enkriptuar të aplikacionit me bazën e të dhënave.	G1. Verifikim teknik dhe evidencat (p.sh. evidenca e kodit të enkriptimit të lidhjes së aplikcaionit me bazë të dhenave.)
H. Realizimi i backup-it të kodit burim dhe testimi i integritetit të backup-it.	H1. Verifikimi teknik dhe evidencat (p.sh. evidencat e pranisë së kopjes së kodit burim dhe testeve për rikuperimin e kodit përmes kopjes së ruajtur)
I. Automatizimi nëpërmjet “pipeline” (“CI/CD” – Continuous Integration / Continuous Delivery /Deployment) integrimit të vazhdueshëm / zhvillim/ implementimit i vazhdueshëm të procesit të zhvillimit, testimit dhe publikimit të softëare-ve.	I1. Verifikimi teknik dhe evidencat vizuale të konfigurimeve dhe funksionimit të CI/CD permes “screenshot”, log-eve dhe dokumentimit të detajuar të parametrave teknike.

B12: Siguria e sistemeve të teknologjisë operacionale (OT)

Të sigurohet mbrojtja e sistemeve të teknologjisë operacionale, duke zbatuar parimin e aksesit minimal, segmentimin e rrjeteve dhe enkriptimin e protokolleve kritike. Të implementohen masa për kontrollin e aksesit, monitorimin në kohë reale dhe mbrojtjen e pajisjeve nga sulmet kibernetike dhe "malëare".

Masa e sigurisë	Implementimi
A. Zbatimi i parimit të privilegjeve të aksesit minimal "Least privileges", duke vendosur kontroll të aksesit të bazuar në role (RBAC) për përdoruesit, Lista e Kontrollit të aksesit ("ACL" - Access Control List") për filtrimin e trafikut, si dhe mbylljen e shërbimeve të panevojshme në sistemet kritike të teknologjisë operacionale (OT)	A1. Verifikimi teknik dhe evidencat.
B. Implementimi i TLS/SSL, VPN për protokollet (MODBUS, IEC 104/105, DNP3, OPC UA, MQTT).	B1. Verifikimi teknik dhe evidenca.
C. Implementimi i teknikave "Hot" dhe "Cold" backups, për ruajtjen e të dhënave.	C1. Verifikimi teknik dhe evidenca
D. Implementimi i nje zgjidhje per menaxhimin e aksesit në distancë, sipas parimit me zero besim (ZTNA).	D1. Verifikimi teknik dhe evidenca
E. Menaxhimi i kontrolluar i patch-eve dhe konfigurimeve, duke e testuar më parë në ambiente testi.	E1 Verifikimi teknik dhe evidenca
F. Implementimi i mbrojtjes se pikave fundore (endpoint), duke përfshirë mekanizmat e detektimit, reagimit apo izolimit të sulmit në nivel "signature" dhe sjelljeje "behaviour".	F1. Verifikimi teknik dhe evidenca
G. Zbatimi i teknikës "Hardening" i pajisjeve të teknologjisë operacionale, si (PLC, RTU, HMI, SCADA, BMS etj)	G1. Verifikimi teknik dhe evidenca
H. Ndarja e infrastrukturës së teknologjisë së informacionit nga teknologjia operacionale (duke siguruar shërbime të veçanta për çdo infrastrukturë, si "Active Directory", "Antivirus", mur mbrojtës i gjeneratës së re ("NextGen Fireëall") dhe SIEM, që janë të dedikuara për teknologjinë operacionale.	H1. Verifikimi teknik dhe evidenca.
I. Implementimi i monitorimit në kohë reale i veprimeve operacionale në sistemet e teknologjisë operacionale, si dhe regjistrimi, analiza dhe njoftimi i	I1. Verifikimi teknik dhe evidenca.

ngjarjeve bazuar në funksionet e rëndësinë e tyre për operacionet kritike.	

B13: Siguria e sistemeve “IoT – Internet of Things”

Të hartohen e të zbatohen procedura për sigurinë e pajisjeve “IoT”, duke përfshirë përdorimin e mekanizmave që garantojnë integritetin dhe konfidencialitetin e sistemeve. Të implementohen azhurnime të sigurta dhe të sigurohet mbrojtja e çelësave të autentifikimit në pajisjet “IoT”.

Masa e sigurisë	Implementimi
A. Hartimi, miratimi, zbatimi dhe rishikimi në mënyrë periodike i procedurave për sigurinë e pajisjeve dhe sistemeve “IoT”.	A1. Procedura për sigurinë e pajisjeve dhe sistemeve “IoT”.
B. Siguria e pajisjeve “IoT”: - Përcaktimi i kërkesave minimale për pajisjet “hardëare”. - Përdorimi i mekanizmave që garantojnë integritet (“tamper proof”) dhe konfidencialitet (Trusted Platform Module). -Aplikimi i azhurnimeve/përditësimeve të sigurta të sistemeve të operimit dhe “firmëare”. - Garantimi i sigurisë së çelësave të autentifikimit. - Kryerja e analizave të trafikut në nivel sjellje (kur aplikohet).	B1. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes “screenshot”, log-eve dhe dokumentimit të detajuar të parametrave teknikë).
C. Garantimi i integritetit dhe konfidencialitetit të të dhënave të transmetuara ndërmjet pajisjeve “IoT”. - Përdorimi i certifikatave autentifikimi që ofrojnë siguri (pajisjet me Hub ose Central “IoT”). - Garantimi i komunikimit të sigurt (TLS 1.2 e lart). - Sigurimi i të dhënave të “IoT” kur transmetohen dhe ruhen. - Përcaktimi i qartë i kontrolleve të aksesit (“IoT hub” dhe aplikimit “IoT Central”). - Realizimi i monitorimit të sigurisë së zgjidhjeve “IoT”.	C1. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes “screenshot”, log-eve dhe dokumentimit të detajuar të parametrave teknikë).

B14: Siguria në sherbimet Cloud

Siguria në shërbimet “Cloud” përfshin masat dhe politikat që sigurojnë mbrojtjen e të dhënave e të shërbimeve të infrastrukturës, duke përfshirë autentifikimin e fuqishëm, enkriptimin e të dhënave dhe monitorimin e aktiviteteve. Këto masa synojnë të garantojnë integritetin,

disponueshmërinë dhe konfidencialitetin e sistemeve të përdorura në “Cloud”, si dhe përputhshmërinë me kërkesat teknike dhe marrëveshje për nivelin e shërbimit (“SLA”- Service Level 14 Agreement) e dakorduara me ofruesit e shërbimeve.

Masa e sigurisë	Implementimi
A. Vendosja e një politike/procedure të qeverisjes për shërbimet në “Cloud”.	A1. Politika/procedura për sigurinë në “Cloud”.
B. Përfshirja e kërkesave teknike, organizative dhe të sigurisë në marrëveshjet e nivelit të shërbimit (SLA) me ofruesit e shërbimeve “Cloud”.	B1. Dokumenti i marrëveshjes për nivelin e shërbimit (SLA), që përfshin indikatorët kryesorë të performancës, metrikat e monitorimit, sigurisë dhe rikuperimit.
C. Implementimi i autentifikimit të fuqishëm, si autentifikimi me shumë faktorë (MFA) për aksesin e platformës së administrimit dhe shërbimeve në “Cloud”.	C1. Verifikimi dhe evidencat për implementimin e autentifikimit në “Cloud”.
D. Implementimi i një mekanizmi enkriptimi për të dhënat në ruajtje dhe në transit.	D1. Verifikim teknik dhe evidenca.
E. Realizimi i kopjes rezervë (backup) të rregullt të shërbimeve kritike dhe të rëndësishme në “Cloud”	E1. Verifikim teknik dhe evidenca.
F. Realizimi i aktivizimit të log-eve dhe monitorimi i aktiviteteve të infrastrukturës në “Cloud”	F2. Verifikim teknik dhe evidenca.
G. Implementimi i një arkitekture të sigurisë së rrjetit që kombinon funksionet e rrjetit dhe sigurisë së teknologjisë së informacionit në një platformë të unifikuar, të bazuar në “Cloud”. Përdorimi i shërbimit të sigurt për aksesin në skaj të rrjetit (“SASE” – Secure Access Service Edge).	G1. Verifikim teknik i zgjidhjes të shërbimit të sigurt për aksesin në skaj të rrjetit (SASE). ii.Verifikimi dhe evidenca e përdorimit të shërbimit të sigurt për aksesin në skaj të rrjetit (SASE) nga përdoruesit