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 për Këshillim Publik me Vendim të Këshillit Drejtues nr. 24, datë 03.11.2025)

RREGULLORE

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

Neni 1
Qëllimi

Kjo rregullore përcakton detyrimin e sipërmarrësve që operojnë për ofrimin e rrjeteve dhe/ose shërbimeve publike të komunikimeve elektronike, që të marrin masat e duhura teknike, organizative dhe proporcionale për të parandaluar dhe minimizuar ndikimin e aksidenteve të sigurisë për përdoruesit e rrjeteve të ndërlidhura.

Neni 2
Objekti

Rregullorja synon të përcaktojë:

a. Objektivat dhe masat për garantimin e funksionimit të infrastrukturës së rrjetit dhe/ose shërbimeve të komunikimit elektronik nga sipërmarrësit që ofrojnë akses në rrjetet e komunikimit publik dhe /ose në shërbimet e komunikimit publik, n ërespekt te konfidencialitetit, integritetit dhe ofrimit te panderprere te sherbimeve.
b. Detyrimet dhe masat bazë që sipërmarrësit duhet të ndërmarrin për të minimizuar apo parandaluar ndodhjen e incidenteve të sigurisë në rrjetet dhe/ose sherbimet e komunikimeve elektronike, dhe për ti raportuar ato nese ndodhin.
c. Kushtet që duhet të plotësojë një cenim ose incident sigurie, në menyrë që të lindë detyrimi i sipërmarrësit për të informuar AKEP 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.
e. Mënyrën dhe përmbajtjen e raportimit të masave të sigurisë dhe incidenteve të sigurisë që duhet dorëzuar në AKEP.
f. Aplikimin e sanksioneve, masave administrative në rast se sipërmarrësit dështojnë në përmbushjen e detyrimeve të përcaktuara në këtë rregullore.

Neni 3
Fusha e zbatimit

Kjo rregullore zbatohet për sipërmarrësit që ofrojnë rrjete publike të komunikimeve elektronike dhe/ose të shërbimeve të komunikimeve elektronike, të disponueshme për publikun, në territorin e Republikës së Shqipërisë.

Neni 4
Baza ligjore

Rregullorja është hartuar në përputhje me ligjin nr. 54/2024 "Për komunikimet elektronike në Republikën e Shqipërisë".

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. Sipërmarrësit janë të detyruar të kryejnë vlerësimin e impaktit të çdo incidenti sigurie mbi rrjetet dhe/ose shërbimet e komunikimeve elektronike publike, sipas kritereve dhe matricës së vlerësimit të paraqitur në Aneksin 2 të kësaj rregulloreje. Tabela e vlerësimit të impaktit duhet të riplotësohet sa herë që ka ndryshime domethënëse në parametrat kryesorë të incidentit.
2. Në vlerësimin përfundimtar të impaktit, nëse të paktën një parametrat e Ankesit 2, e klasifikon incidentin me impakt të lartë, atëherë incidenti konsiderohet incident me impakt të lartë.
3. Brenda 30 (tridhjetë) ditëve pune nga përfundimi i incidentit të sigurisë, sipërmarrësit janë të detyruar të dorëzojnë në AKEP, një vlerësim përfundimtar të impaktit të incidentit, i cili duhet të përmbajë të dhëna të verifikuara dhe masat e marra për reduktimin e pasojave.

Neni 7
Masat për rritjen e sigurisë së rrjeteve

1. Me qëllim parandalimin dhe minimizimin e ndikimit të incidenteve të sigurisë, sipërmarrësit e rrjeteve dhe të shërbimeve të komunikimeve elektronike publike, janë të detyruar
   a. Të kenë rregullore të brendshme për sigurinë, të miratuara, publikuara dhe të përditësuara rregullisht.
   b. Të përgatisin dhe zbatojnë planin e vazhdimësisë së shërbimit, i cili aktivizohet menjëherë në rast incidenti sigurie.
   c. Të publikojnë në faqen e tyre të internetit udhëzues për përdoruesit mbi incidentet më të zakonshme të sigurisë, masat parandaluese dhe veprimet që duhen ndjekur pas ndodhjes së incidenteve.
   d. Të caktojnë të paktën një person të autorizuar përgjegjës për monitorimin e zbatimit të detyrimeve të sigurisë dhe për komunikimin me AKEP në rast incidentesh.
2. Mbajtur parasysh përcaktimet e pikës 1, masat e tjera të detajuara për sigurinë janë sipas Aneksit 3, që i bashkëlidhet kësaj rregulloreje.
3. Të marrin masa mbrojtëse lidhur me të dhënat personale të pëdoruesve:
   a. të sigurojnë që të dhënat personale të jenë të aksesueshme vetëm nga personeli i autorizuar për qëllime specifike ligjore, të përcaktuara qartë dhe të ligjshme;
   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.

4. Sipërmarrësit e komunikimeve elektronike marrin të gjitha masat e nevojshme për të siguruar disponueshmërinë sa më të plotë të shërbimeve të komunikimit zanor dhe shërbimeve të aksesit në internet. Sipërmarrësit që ofrojnë akses në një rrjet publik të komunikimeve elektronike mund të kufizojnë ose të ndërpresin përkohësisht aksesin në shërbimet e tyre, pa miratimin e përdoruesve, nëse kjo është e nevojshme për përmirësimin, modernizimin, mirëmbajtjen ose në rast defektesh apo dëmtimi të rrjetit.

Neni 8
Detyrimet e sipërmarrësve për njoftim në rast incidenti

1. Sipërmarrësit e rrjeteve dhe të shërbimeve të komunikimeve elektronike janë të detyruar të njoftojnë menjëherë AKEP dhe autoritetin përgjegjës për sigurinë kibernetike për incidentin e ndodhur me një impakt të lartë ose mesatar në funksionimin e rrjeteve, sistemeve dhe shërbimeve, sipas formularit në Aneksin 1.

2. Incidenti mund të jetë në një nga format:
   i. Mohimi i marrje së shërbimeve elektronike (DoS/DDoS)
   ii. Kompromet imi i Sistemeve të Informacionit
   iii. Manipulimi ose modifikimi i paautorizuar i të dhënave elektronike
   iv. Software i dëmshëm nën kontrollin e drejtpërdrejtë të sipërmarrësit të komunikimeve elektronike (viruse, spyware, etj.)

3. Sipërmarrësit e rrjeteve dhe të shërbimeve të komunikimeve elektronike publike janë të detyruar të informojnë menjëherë përdoruesit e tyre për një rrezik të veçantë:

a. për 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;

b. në rast të cënimit të të dhënave personale e cila mund të ndikojë keq në të dhënat dhe privatësinë e pajtimtarit.

4. Njoftimi duhet të përshkruajë natyrën e shkeljes së të dhënave personale, caktimin e një personi kontakti në mënyrë që pajtimari të ketë një informacion sa më të detajuar.

5. Në rastet e mosnjoftimit të pajtimtarit nga sipërmarrësi, AKEP, nisur dhe nga ndikimi i shkeljes, i kërkon sipërmarrësit të përmbushë detyrimin lidhur me njoftimin e pajtimtarit.

6. Sipërmarrësit mbajnë regjistër lidhur me shkeljet e të dhënave personale, ndikimin e tyre dhe masat rregullatore të ndërmarra, të mjaftueshme për t'u mundësuar autoriteteve kompetente kombëtare verifikimin e përputhshmërisë lidhur me përmbushjen e detyrimit të njoftimit të pajtimarëve për incidentin e ndodhur.

7. Sipërmarrësit duhet të informojnë AKEP-in dhe të njoftojnë pajtimtarët për kufizimin ose ndërprerjet e shërbimit.

a. 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;

b. 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.

8. Me kërkesë të AKEP, sipërmarrësi:

a. ofron informacion të nevojshëm për të vlerësuar sigurinë dhe integritetin e shërbimeve dhe rrjeteve, duke përfshirë politika të dokumentuara të sigurisë;

b. vë në dispozicion, rezultatet e auditit të sigurisë, të kryer nga një organ i certifikuar dhe i pavarur.

9. Në rast të shkeljes të sigurisë, ose kur rezultatet e auditit sipas pikës 8/b, tregojnë se nuk janë marrë masat e mjaftueshme për sigurinë, AKEP me vendim përcakton masat dhe afatet kohore brenda së cilës sipërmarrësi duhet të ndërmarrë dhe zbatojë këto masa.

Neni 9
Detyrimet e AKEP

1. Lidhur me mbrojtjen e interesave të sigurisë kombëtare dhe garantimin e ruajtjes së integritetit dhe sigurisë së rrjeteve publike të komunikimeve elektronike, AKEP:
   a. informon autoritetin përgjegjës për sigurinë kibernetike në Republikën e Shqipërisë për të gjitha incidentet e sigurisë kibernetike dhe, sipas rastit, informon Komisionin Evropian dhe ENISA-n në përputhje me dispozitat për mbrojtjen e të dhënave.
   b. informon publikun ose u kërkon ofruesve ta bëjnë këtë, kur konstaton se zbulimi i incidentit të sigurisë është në interes të publikut.
   c. shkëmben informacion në lidhje me shkeljen e sigurisë me Komisionin Evropian dhe Agjencinë Evropiane të Rrjeteve dhe Sigurisë së Informacionit (ENISA), si dhe me autoritetet kompetente të vendeve të tjera, në përputhje me kërkesat e ligjit për mbrojtjen e të dhënave për transferimin ndërkombëtar.
   d. bashkëpunon me autoritetin përgjegjës për mbrojtjen e të dhënave personale, për sigurimin e implementimit të politikave të sigurisë lidhur me përpunimin e të dhënave personale.

Neni 10
Raportimi i masave të sigurisë dhe auditimit

1. Sipërmarrësit e komunikimeve elektronike janë të detyruar të paraqesin tek AKEP, informacionin e nevojshëm për vlerësimin e sigurisë së rrjeteve dhe shërbimeve të tyre, përfshirë politikat e sigurisë të dokumentuara,1 (një) herë në vit, jo më vonë se muaji janar për vitin paraardhës, sipas formatit të përcaktuar në Aneksin 3 të kësaj rregulloreje.

2. Pas marrjes së informacionit, nëse AKEP konstaton se të dhënat e raportuara kërkojnë verifikime të thelluara, ka të drejtë t'u kërkojë sipërmarrësve që kanë realizuar të ardhura vjetore nga komunikimet elektronike mbi 100,000,000 lekë në vitin paraardhës, paraqitjen e një Raporti të Auditimit të Sigurisë të kryer nga një organ i pavarur, i certifikuar ose nga autoriteti kompetent shtetëror për sigurinë kibernetike

3. Kostoja e auditimit të sigurisë përballohet në çdo rast nga vetë sipërmarrësi.

4. Në rast se konstatohet se incidenti i sigurisë ka ndodhur pwr shkak tw dobësive strukturore, dhe/ose raporti i auditimit nxjerr në pah masa të pamjaftueshme sigurie, AKEP me vendim, detyron sipërmarrësin të zbatojë masat e sigurisë, duke përcaktuar kërkesat minimale sipas Aneksit 3, dhe afatet konkrete për zbatimin e tyre, sipas Aneksit 4.

Neni 11
Raportimi i Incidenteve të Sigurive

1. Sipërmarrësit janë të detyruar të njoftojnë AKEP-in dhe të dorëzojnë formularin e Aneksit 1 dhe Ankesit 2, jo më vonë se 24 orë nga momenti i evidentimit të incidentit të sigurisë, pas vlerësimit paraprak të impaktit të tij. Njoftimi është i detyrueshëm vetëm në rast se incidenti klasifikohet me impakt mesatar ose të lartë.
2. Njoftimi fillestar duhet të përmbajë minimalisht këto të dhëna:
   a. Vlerësimin mbi rrjetet ose shërbimet e komunikimit publik që janë ndikuar nga incidenti i sigurisë;
   b. Zonën gjeografike të ndikuar ose potencialisht të ndikuar;
   c. Segmentin e përdoruesve të ndikuar dhe/ose të rrezikuar nga incidenti;
   d. Vlerësimin paraprak të shkakut ose shkaqeve që mendohet se kanë sjellë incidentin.
   e. Vlerësimin e planit të rikuperimit dhe masave të marra deri në momentin e raportimit;
3. Nëse pas njoftimit fillestar, ka një ndryshim të rëndësishëm në të dhënat e raportuara, sipërmarrësi është i detyruar të dërgojë menjëherë një njoftim të ri, të përditësuar pranë AKEP.
4. Brenda 10 ditëve pune nga ndodhja e incidentit të sigurisë, sipërmarrësit janë të detyruar të dorëzojnë pranë AKEP-it një njoftim përfundimtar, me të dhëna të plota dhe të verifikuara, duke plotësuar sërish formularin e Aneksit 1, sipas kërkesave të përcaktuara në pikën 2 të këtij neni.
5. Njoftimet sipas këtij neni, dërgohen pranë AKEP, përmes adresës zyrtare të dedikuar incidente.raportimi@akep.al dhe në formë shkresore në AKEP.
6. AKEP mund të kërkojë në çdo kohë informacion shtesë mbi incidentin e sigurisë, përtej të dhënave të përcaktuara në formular. Për këtë arsye, sipërmarrësit janë të detyruar të ruajnë të gjitha të dhënat e lidhura me incidentin për një periudhë jo më pak se 12 muaj, duke filluar nga data e dorëzimit të njoftimit përfundimtar.

Neni 9
Kundërvajtjet administrative

Shkeljet e kësaj rregulloreje, kur nuk përbëjnë vepër penale, konsiderohen kundërvajtje administrative dhe dënohen me gjobë sipas pikës 1, shkronjës a/xii të nenit 184 të ligjit nr. 54/2024 “Për komunikimet elektronike në Republikën e Shqipërisë”.

Neni 10
Shfuqizime

Rregullorja nr. 37 datë 29.10.2015 “Mbi masat teknike dhe organizative per te garantuar sigurine dhe integritetin e rrjeteve dhe/ose sherbimeve te komunikimeve elektronike” shfuqizohet.

Neni 11

Hyrja në fuqi

Kjo Rregullore 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

		○ 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	

Udhëzime për plotësimin dhe dërgimin e formularit:

- Formulari plotësohet brenda 24 orëve nga zbulimi i incidentit.
- Duhet të bashkëngjitet Aneksi 2 (vlerësimi i impaktit) dhe çdo evidencë teknike (log-e, raport analiza, etj.).
- Dokumentacioni i mësipërm, dërgohet në adresën zyrtare të AKEP: incidente.raportimi@akep.al, pasi të jetë nënshkruarnga personi përgjegjës për sigurinë kibernetike pranë sipërmarrësit.

ANEKS 2 – Vlerësimi i impaktit të sigurisë

Parametri	Njësia e matjes / përshkrimi	Impakt i ulët	Impakt mesatar	Impakt i lartë
Kohëzgjatja e ndërprerjes	Koha totale e ndërprerjes ose degradimit të shërbimit	< 1 orë	1 – 6 orë	> 6 orë
Numri i përdoruesve të ndikuar	Numri absolut ose përqindja e përdoruesve të prekur nga incidenti	≤ 0.2 % e totalit ose ≤ 1000 përdorues	0.2 – 5 % e totalit	≥ 5 % ose ≥ 1000 përdorues
Shtrirja gjeografike	Sipërfaqja ku është ndier efekti i incidentit	< 5 km² (zonë lokale)	5 – 20 km² (zonë rajonale)	> 20 km² (zonë kombëtare)
Ndikimi mbi rrjet dhe shërbimet	Nëse incidenti prek shërbime të komunikimeve publike kritike	Asnjë ndikim	Ndikim i kufizuar / i pjesshëm	Ndikim i drejtpërdrejtë në shërbime kritike

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.

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	Dokumentim / Verifikim i implementimit
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	Dokumentim / Verifikim i implementimit

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 trajnimin e rreziqeve të identifikuara.	C1. Dokument i planit për trajnimin 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	Dokumentim / Verifikim i implementimit
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)

A4: Kërkesat e sigurisë kibernetike për palët e treta

Të krijohet e të zbatohet një politike 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.

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 te 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 ndërgjegjësimin e burimeve njerëzore, si dhe të aksesit të personave, në bazë të objektivave të sigurisë në lidhje me personelin.

Masa e sigurisë	Dokumentim / Verifikim i implementimit
A. Vendosja e një politike sigurie për burimet njerëzore.	A1. Politika e sigurisë 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. (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" 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").
D. Testimi i njohurive të punonjësve për sigurinë kibernetike. (Minimumi njëherë në vit, të cilët përdorin sistemet kritike të informacionit në infrastrukture dhe/ose më shpesh në varësi të incidenteve kibernetike)	D1. Pyetësorë dhe rezultate testimi për ndërgjegjësimin e punonjësve në lidhje me sigurinë kibernetike.

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	Dokumentim / Verifikim i implementimit
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	Dokumentim / Verifikim i implementimit
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	Dokumentim / Verifikim i implementimit
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	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

një incidenti kibernetik ("DRS" – Vendi i rikuperimit nga katastrofa/Disaster Recovery Site).	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	Dokumentim / Verifikim i implementimit
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.

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	Dokumentim / Verifikim i implementimit
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.

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	Dokumentim / Verifikim i implementimit
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 sistemeve, si dhe enkriptimi i trafikut me protokolle të sigurta	B1. Verifikimi teknik dhe evidencat për vendosjen e filtrave dhe enkriptimin e trafikut.
C. Kontrolli nëse në fireëall ka të konfiguruar lista të autorizuara/lista të	C1. Verifikim dhe evidenca për konfigurimet në murin mbrojtës digjital (fireëall).

bllokuara (“Ëhitelist/Blacklist”) të adresave të protokollit të internetit (IP) të lejuara ose bllokuara	
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	Dokumentim / Verifikim i implementimit
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	Dokumentim / Verifikim i implementimit
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	Dokumentim / Verifikim i implementimit
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	Dokumentim / Verifikim i implementimit
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	Dokumentim / Verifikim i implementimit
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 fundore(“NAC“- Netëork Access Control)	K1. Procedure për përcaktimin e parametrave të sigurisë minimale(baseline). K2. Verifikim teknik dhe evidencat.

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	Dokumentim / Verifikim i implementimit
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	Dokumentim / Verifikim i implementimit
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 të të dhënave të ndjeshme jashtë infrastrukturës.	B1.Verifikimi i implementimit të metodës për parandalimin e humbjes së të dhënave (DLP) për rrjedhjen e të dhënave të ndjeshme.

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	Dokumentim / Verifikim i implementimit
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. (Minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën	G1. Raporti i testimeve të llojeve: "black", "grey", "ëhite" për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (penetration test) dhe plani i trajtimit.

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	Dokumentim / Verifikim i implementimit
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	Dokumentim / Verifikim i implementimit

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 ngjarjeve bazuar në funksionet e rëndësinë e tyre për operacionet kritike.	I1. Verifikimi teknik dhe evidenca.

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	Dokumentim / Verifikim i implementimit
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	C1. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "screenshot", log-eve dhe dokumentimit të detajuar të parametrave teknikë).

(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".	

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	Dokumentim / Verifikim i implementimit
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

ANEKS 4 – Kategorizimi i nivelit të rrezikut dhe masave korrigjuese

Në këtë aneks parashtrohen matrica e vlerësimit të rrezikut e bazuar në kombinimin e probabilitetit të ndodhjes së ngjarjes me impaktin mbi rrjetin, shërbimin ose asetet kritike.

		Impakti				
		shume i ulet	i ulet	mesatar	i larte	shume i larte
Probabiliteti	shume i ulet	1	2	3	4	5
	i ulet	2	4	6	8	10
	mesatar	3	6	9	12	15
	i larte	4	8	12	16	20
	shume i larte	5	10	15	20	25

Sipas vlerësimit te rrezikut, ne tabelën e mëposhtme paraqiten afatet kohore te përmbushjes se hendeqeve te evidentuara sipas nivelit te rrezikut.

Niveli i rrezikut	Koha e trajtimit
1-5 ,Shume i ulet	Nuk ka nevoje per trajtim
6-10, I ulet	Nuk ka nevoje per trajtim
11-15, Mesatar	Ka nevoje per trajtim brenda afatit kohor prej 12 muajsh.
16-25, I larte	Ka nevoje per trajtim brenda afatit kohor prej 6 muajsh.