REPUBLIKA E SHQIPËRISË
KËSHILLI I MINISTRAVE
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

RREGULLORE

MBI

MËNYRËN E DOKUMENTIMIT DHE IMPLEMENTIMIT TË MASAVE TË SIGURISË NË INFRASTRUKTURAT KRITIKE DHE TË RËNDËSISHME TË INFORMACIONIT

V3.0

Miratuar me Urdhrin Nr. 97 datë 05.03.2024

QËLLIMI

Në zbatim të Ligjit Nr. 2/2017, "Për Sigurinë Kibernetike", Vendimit të Këshillit të Ministrave Nr. 141, datë 22.2.2017, "Për organizimin dhe funksionimin e Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike" si dhe Vendimit të Këshillit të Ministrave Nr. 553, datë 15.07.2020 "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit"e ndryshuar, AKCESK, me qëllim arritjen e një niveli të lartë të sigurisë kibernetike, duke përcaktuar masat e sigurisë, të drejtat, detyrimet, si dhe bashkëpunimin e ndërsjellë ndërmjet subjekteve që operojnë në fushën e sigurisë kibernetike, në përmbushje të detyrave specifike do të kontrollojë infrastrukturat kritike te rëndësishme te informacionit. Për sistemet dhe rrjetet kritike të informacionit janë të detyrueshëm dy nivelet e sigurisë, për sistemet dhe rrjetet e rëndësishme të informacionit është i detyrueshëm vetem niveli i parë i sigurisë.

OBJEKTI

Kontrolli i Operatorit të Infrastrukturës Kritike dhe të Rëndësishme të Informacionit do të realizohet sipas Programit më poshtë.

Programi liston 20 objektiva sigurie, duke u ndarë në Masa Teknike dhe Masa Organizative mbështetur mbi standardet ndërkombëtare.

Për secilin nga objektivat e sigurisë listohen masa më të detajuara të sigurisë, së bashku me mënyrën e dokumentimit të tyre. Masat e sigurisë dhe mënyra e dokumentimit përbëjnë listën e kërkesave minimale për OIKI dhe OIRI.

STRUKTURA E MASAVE TË SIGURISË KIBERNETIKE

Për secilin nga objektivat e sigurisë listohen masa sigurie më të detajuara të cilat duhet të implementohen nga operatorët për të arritur objektivin e sigurisë kibernetike. Për secilin nga objektivat e sigurisë gjithashtu listojmë dokumentime ose evidenca të detajuara që mund të tregojnë se masat janë implementuar dhe janë në fuqi.
Masat e sigurisë kibernetike grupohen në 2 (dy) nivele, si më poshtë:

NIVELI I SIGURISË	Përshkrimi i niveleve të sigurisë
1	Niveli 1 (Masat që janë të detyrueshme për OIRI dhe OIKI) Masa sigurie të nivelit të ulët dhe të mesëm duhen implementuar për të arritur objektivat e sigurisë. Dokumentimi që masat e sigurisë të nivelit të ulët dhe të mesëm janë implementuar. Masat e sigurisë të nivelit të ulët dhe të mesëm për të arritur objektivin dhe një rishikim ad-hoc të zbatimit, pas ndryshimeve apo incidenteve. Dokumentimi i masave të sigurisë së nivelit të ulët dhe të mesëm dhe dokumentimin e rishikimeve të zbatimit pas ndryshimeve ose incidenteve.
2	Niveli i dytë (Masat që janë të detyrueshme për OIKI) Masa sigurie në nivel të lartë dhe monitorimin e vazhdueshëm të zbatimit, rishikimin e zbatimit, duke marrë parasysh ndryshimet, incidentet, testet dhe ushtrimet, për të përmirësuar në mënyrë pro - aktive zbatimin e masave të sigurisë. Dokumentimi i zbatimit të avancuar të masave të sigurisë, dokumentimi i një procesi të shqyrtimit strukturor dhe dokumentimi i hapave pro - aktiv për të përmirësuar zbatimin e masave të sigurisë.

Niveli i parë i masave të sigurisë duhet implementuar dhe dokumentuar nga Operatorët e Infrastrukturave të Rëndësishme të Informacionit, ndërsa niveli i dytë, përfshirë nivelin e parë, duhet implementuar dhe dokumentuar nga Operatorët e Infrastrukturave Kritike të Informacionit.

MASAT E SIGURISË KIBERNETIKE

Më poshtë listohen 20 masa sigurie të nivelit të ulët, të mesëm dhe të lartë, (MS1, MS2, etj.), të grupuara në 2 kategori (K1, K2). Për secilën kategori të masave të sigurisë, listohen masat e sigurisë të detajuara, të cilat duhet të implementohen nga operatorët, po ashtu edhe llojin e dokumenteve që do të merren në konsideratë.

K1: MASAT ORGANIZATIVE

MS1: Politika e sigurisë
MS2: Menaxhimi i riskut
MS3: Siguria organizative
MS4: Kërkesat e sigurisë për palët e treta
MS5: Siguria e burimeve njerëzore dhe aksesit të personave
MS6: Menaxhimi i Aseteve
MS7: Ngjarjet e sigurisë dhe menaxhimit të incidenteve të sigurisë kibernetike
MS8: Menaxhimi i vazhdimësisë së punës
MS9: Menaxhimi i sigurisë së informacionit
MS10: Kontrolli dhe auditi

K2 : MASAT TEKNIKE

MS1: Siguria fizike
MS2: Menaxhimi për autorizimin e aksesit
2.2.1 Ndërgjegjësimi ndaj kërcënimit
MS3: Pajisjet kriptografike
MS4: Zbulimi i ngjarjeve të sigurisë kibernetike
MS5: Mjetet e gjurmimit dhe vlerësimit të ngjarjeve të sigurisë kibernetike
MS6: Mbrojtja e integritetit të rrjeteve të komunikimit
MS7: Verifikimi i identitetit të përdoruesve
MS8: Veprimtaria e administratorëve dhe përdoruesve
MS9: Siguria e aplikacioneve
MS10: Siguria e sistemeve industriale

1. MASAT ORGANIZATIVE

1.1. MS1: Politika e sigurisë

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

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të vendoset një politikë sigurie e nivelit të lartë e miratuar nga stafi i lartë menaxhues që adreson sigurinë e rrjeteve të komunikimit dhe sistemeve të informaconit, dhe të rishikohet në mënyre periodike.	i. Politika e sigurisë dhe objektivat e sigurisë së informacionit.	

1.2. MS2: Menaxhimi i rrezikut kibernetik

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

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Krijimi i një metodologjie për menaxhimin e rrezikut. b) Të bëhet një listë e rreziqeve për sigurinë e rrjeteve të komunikimit dhe sistemeve të informacionit, duke marrë në konsideratë kërcënimet kryesore për asetet kritike dhe të rishikohet në mënyre periodike. c) Të hartohet një plan për trajtimin e risqeve.	i. Metodologji e dokumentuar e menaxhimit të rrezikut. ii. Lista e vlerësimit të rreziqeve duke përfshirë dhe rreziqet të cilat vijnë nga palët e treta. iii. Plani i trajtimit të rreziqeve.	

1.3. MS3 : Siguria organizative

Të krijohet dhe mbahet një strukturë e përshtatshme e roleve të sigurisë dhe përgjegjësive.

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të caktohen rolet e sigurisë dhe përgjegjësitë.	i. Listë e roleve të sigurisë, përshkrimi i përgjegjësive dhe detyrave, informacione kontakti dhe si/kur duhet të kontaktohen.	

1.4. MS4: Kërkesat e sigurisë kibernetike për palët e treta

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

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të vendoset një politikë sigurie për kontratat me palët e treta dhe të rishikohet në mënyrë periodike. b) Të përfshihen kërkesat e sigurisë në kontratat me palët e treta, duke përfshirë konfidencialitetin dhe transferimin e sigurt të informacionit.	i. Politika e sigurisë për kontratat me palët e treta. ii. Kërkesa të qarta sigurie në kontratat me palët e treta. iii. Marrëveshje konfidencialiteti për ruajtjen e informacionit me palët e treta.	
2	c) Të mbahen gjurmët/rekordet e incidenteve të sigurisë kibernetike që lidhen ose janë të shkaktuara nga palët e treta.	iv. Lista e incidenteve të sigurisë kibernetike që lidhen ose janë të shkaktuara nga angazhimi me palët e treta.	

1.5. MS5 : Siguria e burimeve njerëzore dhe aksesit të personave

Siguria e burimeve njerëzore dhe aksesit të personave mbulon objektivat e sigurisë në lidhje me personelin.

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të vendoset një politikë sigurie për burimet njerëzore, e cila mbulon ciklin e plotë të punësimit duke përfshirë fazat para rekrutimit, gjatë punësimit, përfundimi apo ndryshimi i marrëdhënies së punës, proceset disiplinore, mbrojtja e te dhënave personale. b) Të implementohet një program trajnimi, duke u siguruar që personeli të ketë njohuri të mjaftueshme dhe të përditësuara për sigurinë kibernetike sipas profilit të punës. c) Të informojë dhe trajnojë personelin e ri mbi politikat dhe procedurat në fuqi.	i. Politika e sigurisë së burimeve njerëzore. ii. Dokumenti i kontrolleve të referencave profesionale të personelit kryesor. iii. Dokument i realizimit të fushatave të ndërgjegjësimit të punonjësve në lidhje me sigurinë kibernetike dhe sulmet më të shpeshta si Phishing etj.	
2	d) Të testohen njohuritë e personelit mbi sigurinë kibernetike.	iv. Rezultatet e testeve.	

1.6. MS6: : Menaxhimi i aseteve

Të krijohen dhe mbahen procedurat e menaxhimit të aseteve dhe kontrollet e konfigurimit në mënyrë që të menaxhohet disponueshmëria e aseteve kritike dhe konfigurimet e rrjeteve të komunikimit dhe sistemeve të informacionit.

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të merren masa për identifikimin dhe menaxhimin efektiv të aseteve duke evidentuar: -Vjetërsisë -Afektimin e C/I/A -Vulnerabilitetet e identifikuara (CVE). b) Të vendosen politika/procedura për menaxhimin e aseteve, duke përfshirë rolet dhe përgjegjësitë, asetet dhe konfigurimet që janë objekt i politikës, objektivat e menaxhimit të aseteve, si dhe shkatërrimin e aseteve. c) Të merren masa për zëvendësimin ose izolimin e sistemeve “End of Life” të instaluara në pajisjet tuaja. d) Të realizohen patch-ime automatike në sistemet fundore (patch-et e sistemeve të operimit, antivirusit).	i. Inventari i aseteve të sigurisë së informacionit për IT/OT. ii. Politika/procedura e menaxhimit të aseteve. iii. Politika e Clean Desk dhe politika e kyçjes së ekranit pas një kohe idle. iv. Topologji e detajuar e rrjetit dhe sistemeve të informacionit. v. Verifikimi i sistemeve dhe evidencat. vi. Verifikimi i sistemeve të patch-imeve për pajisjet fundore dhe antivirusin dhe evidencat.	
2	e) Të ndiqen metodat, procedurat dhe politikat kur bëhen ndryshime. f) Të vendosen procedurat operacionale dhe të caktohen përgjegjësitë për funksionimin e sistemeve kritike.	vii. Procedura e menaxhimit të ndryshimeve. viii. Procedura operacionale.	

1.7. MS7: Ngjarjet e sigurisë e të menaxhimit të incidenteve të sigurisë kibernetike

Ngjarjet e sigurisë e të menaxhimit të incidenteve të sigurisë kibernetike përfshijnë zbulimin, reagimin, raportimin dhe komunikimin e incidentit kibernetik.

	Masat e sigurisë	Dokumentimi/Verifikimi I implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të hartohen plane dhe procedura të detajuara për menaxhimin e incidenteve kibernetike. b) Të mbahen rekorde për të gjitha incidentet të sigurisë kibernetike dhe për secilin, ndikimi, shkaku, veprimet e marra dhe mësimet e nxjerra. c) T’u komunikohen dhe raportohen incidentet kibernetike aktuale ose të mëparshme palëve të treta, klientëve dhe/ose autoriteteve qeveritare, kur është e nevojshme.	i. Procedurat dhe planet. ii. Inventari i incidenteve kibernetike. iii. Raporte individuale për trajtimin e incidenteve kibernetike. iv. Formulari i raportimeve të incidenteve kibernetike.	

1.8. MS8: Menaxhimi i vazhdimësisë së punës

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

		Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të implementohet një strategji për vazhdimësinë e shërbimit për rrjetet e komunikimit dhe sistemet e informacionit duke përfshirë kohën e rikuperimit, skenarët e incidenteve/katastrofave dhe personat përgjegjës për shërbimet dhe proceset kryesore. b) Të merren masa për shfrytëzimin e teknikave të pasqyrimit të të dhënave (RAID 1/5/6/10) për të shmangur humbjen e të dhënave sensitive. c) Të realizohet nje politikë për kryerjen e backup-eve duke përfshirë frekuencat, llojet, të dhënat dhe shërbimet. d) Të realizohen backup-e duke përdorur teknika me karakteristikën Backup Lock Retention ose me Tape në formatin Worm dhe të testohet integriteti i tyre	i. Strategjia e dokumentuar e vazhdimësisë së shërbimit. ii. Politika e backup. iii. Verifikimi i konfigurimeve të RAID dhe evidencat. iv. Raporte të testimit të planeve rezervë (backup) dhe testimit të integritetit të tyre.	
2	a) Të merren masa për shmangien e "Single Point of Failure" tek shërbimet tuaja kritike dhe të rëndësishme. b) Të merren parasysh skemat "High-Availability" në pajisjet "core-network" në nivel perimetri (firewall), në nivel rutimi (L3) dhe komutimi paketash (L2) dhe nivel linjash fizike (L1). c) Të implementohet Disaster Recovery Site për shërbimet më të rëndësishme dhe kritike.	v. Verifikimi i Single Point of Failure dhe evidencat. vi. Raporte të testimit të DRS të skenarëve të incidenteve/katastrofave.	

1.9. MS9: Menaxhimi i sigurisë së informacionit

Të krijohet dhe mbahet një politikë për monitorimin e pajtueshmërisë së standardeve me kërkesat ligjore

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të monitorohet pajtueshmëria e standardeve me kërkesat ligjore. b) Të implementohen politika/procedurat për monitorimin e pajtueshmërisë dhe auditimit.	i. Raportet e monitorimit të pajtueshmërisë. ii. Politika/procedura të dokumentuara.	

1.10. MS10: Kontrolli dhe auditi

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Politikë/procedurë për kontrollin dhe auditin e brendshëm dhe rishikimi në mënyrë periodike. b) Të kryhen kontrolle/audite të brendshme ose nga palët e treta për sigurinë e informacionit në infrastrukturat tuaja.	i. Politika/Procedura e auditit të brendshëm. ii. Raporti i auditit dhe plani i trajtimit.	

2. MASAT TEKNIKE

2.1 MS1: Siguria fizike

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

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të Implementohen masat e sigurisë fizike dhe kontrolleve mjedisore, si bravat e dyerve dhe kabineteve, kontrolli elektronik i hyrjes dhe log-et e auditimit, segmentimi i hapësirave sipas niveleve të autorizuara alarmi i aksesit të paautorizuar, alarmet e zjarrit, fikësit e zjarrit, fikësit e automatizuar të zjarrit me gaze halokarbonike etj. b) Implementimi i një politike për masat e sigurisë fizike dhe kontrollet mjedisore dhe rishikimi në mënyrë periodike.	i. Raportet e testimit. ii. Politika e sigurisë fizike.	

2.2. MS2: Menaxhimi për autorizimin e aksesit

Krijoni dhe mbani kontrolle aksesi të duhura (logjike) për të aksesuar rrjetet e komunikimit dhe sistemet e informacionit.

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)

1	a) Implementimi i politikave për mbrojtjen e aksesit në rrjetet dhe sistemet e informacionit e cila përfshin përshkrimin e roleve, grupeve, të drejtave të aksesit, procedurat për dhënien dhe revokimin e aksesit, si dhe mos përdorimin e llogarive gjenerike (*generic account*). b) Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë). c) Të kontrollohen nëse në firewall ka të ngritur Whitelist të adresave te lejuara IP. d) Te përdoret politika e password-eve rastesorë për userat/administratorët local (Psh si LAPS te Microsoft).	i. Politika e kontrollit të aksesit ii. Formular për dhënie të drejtash aksesi. iii. Formular për revokim të drejtash aksesi dhe dorëzimi asetesh. iv. Verifikimi dhe evidencat v. Verifikimi dhe evidencat	
2	e) Të projektohet zgjidhja për menaxhimin e aksesit të përdoruesve "Identity Access Management" për të kontrolluar identitetin dhe privilegjet e përdoruesve në kohë reale sipas parimit "zero-trust".	vi. Raporte të monitorimit të llogarive të përdoruesve.	

2.2.1. Ndërgjegjësimi ndaj kërcënimit kibernetik

Të krijohet dhe mbahet një mekanizëm për monitorimin dhe mbledhjen e informacionit në lidhje me kërcënimet përkatëse të sigurisë së rrjeteve të komunikimit dhe sistemeve të informacionit.

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të kryhet monitorim i vazhdueshëm i burimeve të jashtme të "threat intelligence" (OSINT) të kërcënimeve kibernetike.	i. Raporte monitorimi	
2	b) Të zbatohet programi i "threat intelligence" që përfshin rolet, përgjegjësitë, procedurat dhe mekanizmat për mbledhjen e informacionit lidhur me kërcënimet e rëndësishme dhe masat parandaluese përkatëse.	ii. Programi i dokumentuar dhe ndarja e informacionit.	

2.3. MS3: Pajisjet kriptografike

Të sigurohet përdorimi adekuat i enkriptimit për të parandaluar dhe/ose minimizuar impaktin e incidenteve të sigurisë kibernetike tek përdoruesit, në rrjetet e komunikimit dhe sistemet e informacionit.

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të Implementiohet politika e enkriptimit duke përfshirë detaje rreth algoritmeve kriptografike (AES, RSA, ECC, TLS, IPSec, SSH, etj.) dhe çelësave kriptografikë.	i. Politika e enkriptimit	

2.4. MS4: Zbulimi i ngjarjeve të sigurisë kibernetike

Të krijohen dhe mbahen kapacitete për zbulimin e incidenteve të sigurisë kibernetike që identifikojnë incidentet.

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të implementohet sistem i automatizuar për menaxhimin dhe filtrimin e log-eve me qëllim identifikimin e alerteve në kohë reale (SIEM).	i. Kontrolli teknik dhe evidencat.	

2.5. MS5: Mjetet e gjurmimit të vlerësimit të ngjarjeve të sigurisë kibernetike

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

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të implementohet politika për monitorimin dhe regjistrimin, duke përfshirë kërkesat minimale për monitorimin dhe regjistrimin, periudhën e mbajtjes, objektivat e përgjithshme të ruajtjes, monitorimit të të dhënave dhe log-et. b) Të vendosen mjete për mbledhjen e log-eve të sistemeve kritike.	i. Politika e monitorimit dhe rregjistrimit. ii. Raporte/Evidenca te ruajtjes dhe monitorimit të log-eve të rrjetit kritik dhe të sistemeve të informacionit.	

2.6. MS6: Mbrojtja e integritetit të rrjeteve të komunikimit

Të krijohet dhe ruhet integriteti i rrjeteve dhe sistemeve të informacionit dhe të mbrohen nga viruset, injeksionet e kodeve dhe malware-ve të tjera që mund të ndryshojnë funksionalitetin e sistemeve.

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)

1	a) Të instalohen pajisje të perimetrit të rrjetit që bëjnë analizë të thellë të trafikut duke u mbështetur jo vetëm në rregullat e listave të aksesit por edhe në sjelljen e tij (Next Generation Firewall). b) Të kryhen analiza të trafikut në nivel sjellje "behaviour" për pajisjet fundore. c) Të verifikohet ndarja e rrjetit në nën-rrjete. d) Të vendosen në zona/subnet/vlan të ndryshme kompjuterat e përdoruesve me Serverat dhe të kontrollohen me akses lista. e) Të merren masa për izolimin e rrjetit wireless nga pjesa tjetër e rrjetit. f) Të përdoret teknika e Port Security te Switch-et ku numri maksimal i MAC Adresave të jetë 1 për përdoruesit e thjeshtë dhe një numer i limituar për ekspertët e IT-së ose Sigurisë Kibernetike. g) Të sigurohet që sistemet kritike t'u nënshtrohen rregullisht skanimeve të sigurisë dhe testeve të sigurisë, veçanërisht kur kemi përdorimin e sistemeve të reja dhe ndryshime. h) Te merren masa për fortifikimin (hardening procedure) e te gjitha pajisjeve që janë pjesë e rrjetit (pc, server ,Switch, Router,Firewall, etj) i) Të izolohen logjikisht (në VLAN të ndryshëm) Database dhe Web service-t (nëse janë të hostuara në ambjentin tuaj).	i. Verifikimi teknik dhe evidencat. ii. Raporte nga skanimet dhe testet e mëparshme të sigurisë. iii. Verifikimi teknik dhe evidencat.	
2	j) Të merren masa për ngritjen e DNS_SEC për të shmangur DNS_Amplification attack dhe DNS_Poisoning attack. k) Të përdoret teknika e mbrojtjes ndaj DoS/DDoS attack. l) Të merren masa për implementimin e një sistemi që kontrollon parametrat e sigurisë së një sistemi fundor, duke mos e lejuar këtë të fundit të jetë pjesë e rrjetit tuaj nëse këto parametra janë nën nivelin "baseline" të dhënë më parë nga ju.	iii. Verifikimi teknik dhe evidencat.	

2.7. MS7: Verifikimi i identitetit të përdoruesve

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të implementohet politika për menaxhimin e fjalëkalimeve të përdoruesve. b) Metoda të përcaktuara për dhënien e aksesit të përdoruesve (Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-based Access Control (RBAC) etj. c) Të merren masa për menaxhimin e akseseve, politikave, privilegjeve të userave nëpërmjet Active Directory (AD)	i. Politika për menaxhimin e fjalëkalimeve. ii. Verifikimi dhe evidencat.	
2	d) Implementimi i sistemeve me 2 Faktorë Autentifikimi (2FA) në nivel aplikacioni/web/mail/pajisje për të gjithë përdoruesit.	iii. Verifikimi dhe evidencat.	

2.8. MS8: Veprimtaria e administratorëve dhe përdoruesve

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Implementimi i sistemeve me 2 Faktorë Autentifikimi (2FA) në nivel aplikacioni/web/mail/pajisje për administratorët.	i. Verifikimi dhe evidencat.	
	a) Të përdoret platforma Data Leakage Prevention për parandalimin e rrjedhjes se informacionit.	ii. Verifikimi dhe evidencat.	

2.9 MS9: Siguria e aplikacioneve

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të kryhen testime për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (vulnerability assessment - VA) dhe të hartohet plani për trajtimin e problematikave të evidentuara. b) Të kontrollohen nese ka Web Service që operon në protokollin http. c) Të konfigurohen feature-at anti-spoofing: DMARC/SPF/DKIM në sistemin e Email-it. d) Nëse keni një departament zhvillimi, të realizohen testime të zhvillimeve të software-ve (stage-ing) në	i. Raporti i vlerësimit të vulnerabiliteteve (vulnerability assessment - VA) dhe plani i trajtimit. ii. Verifikimi teknik dhe evidencat.	

	ambient të izoluar të ndarë nga ambienti i prodhimit (production).	iii. Verifikimi i zonave/segmenteve të rrjetit.	
2	e) Të implementohen zgjidhje që kryen filtrimin, monitorimin dhe bllokimin e trafikut keqdashës ndërmjet aplikacioneve Web dhe internetit, Web Application Firewall (WAF). f) Të implementohet Reverse Proxy. g) Të kryhen testime për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (Penetration Test – Black Gray dhe opsion White) dhe të hartohet plani për trajtimin e problematikave të evidentuara.	iv. Verifikimi teknik dhe evidencat. v. Raporti i testimit për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (penetration test) dhe plani i trajtimit.	

5.10 MS10 Siguria e sistemeve industriale (OT)

	Masat e sigurisë	Dokumentimi/Verifikimi i implementimit	PO/JO/Në proces/E pa aplikueshme (emërtimi i dokumentit, versioni, data)
1	a) Të ndahet infrastruktura OT nga IT (secila infrastrukturë me shërbime të ndara, si për shembull Active Directory, Antivirus, Firewall, SIEM etj.). b) Të merren masa për zbatimin e parimit “Least privileges” duke vendosur RBAC për përdoruesit, ACL për filtrimin e trafikut, si dhe mbylljen e shërbimeve të pa nevojshme. c) Të realizohet segmentimi në zona për OT (psh. zona Production, zona DMZ, zona e menaxhimit etj.) d) Të implementohet teknika Cold Backup. e) Të mbyllet ose implementohet një zgjidhje e sigurtë dhe e kontrolluar sipas parimit zero-trust i aksesit në distancë. f) Të implementohet zgjidhja Failover-Protection. g) Të realizohet menaxhimi i kontrolluar i patch-eve dhe konfigurimeve duke u testuar më pare në ambjente testi. h) Të realizohet kontrolli i software për zonën production (Application Whitelisting manual ose automatik). i) Të merren masa për monitorimin dhe njoftimin në kohë reale të veprimeve operacionale (OT operational monitoring) bazuar në funksionet e tyre.	i. Verifikimi teknik dhe evidencat	

	j) Të merren masa për implementimin e endpoint protection duke përfshirë mekanizmat e detektimit, reagimit apo izolimit të sulmit në nivel “signature” dhe sjelljeje “behaviour”.		