REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Rregullore mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë

Miratuar me Urdhrin nr.22, datë 26.04.2018 të Drejtorit të Përgjithshëm të Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)

Përmbajtje

Hyrje

Kjo rregullore është hartuar në bazë të Ligjit Nr. 2, datë 26.01.2017, "Për Sigurinë Kibernetike", Neni 9, pika 2 dhe pika 3.

Qëllimi

Qëllimi i hartimit të kësaj rregulloreje është arritja e një niveli të lartë të sigurisë kibernetike, duke përcaktuar masat e sigurisë, të drejtat, detyrimet për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe përcakton përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë.

Fusha e zbatimit

Zbatimi i kësaj rregullore është i detyrueshëm për të gjithë Operatorët e Infrastrukturave Kritike të Informacionit dhe Operatorët e Infrastrukturave së rëndësishme të informacionit të listuara në VKM Nr. 222, datë 26.04.2018, " Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit"

Informacion i përgjithshëm

Kjo rregullore synon të përcaktojë objektivat dhe masat për garantimin dhe funksionimin e sistemeve të informacionit dhe rrjetet e komunikimit në Operatorët e Infrastrukturës Kritike të Informacioni (OIKI) dhe Operatorët e Infrastrukturës së Rëndësishme të Informacionit (OIRI).

Rregullorja përcakton gjithashtu detyrimet dhe masat bazë që OIKI dhe OIRI duhet të ndërmarrin për të minimizuar apo parandaluar incidentet e sigurisë në rrjetet e komunikimit dhe sistemet e informacionit, si dhe përcakton standardizimin në vlerësimin dhe raportimin e incidenteve dhe masave të sigurisë.

Rregullorja liston 20 objektiva sigurie, duke u ndarë në Masa teknike dhe organizative, mbështetur mbi standardet ndërkombëtare që përdoren nga ofruesit e sektorit të komunikimit elektronik në BE. 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.

Përkufizime

"Operator i infrastrukturës kritike të informacionit" (OIKI) është një person juridik, publik ose privat, që administron infrastrukturën kritike të informacionit.

"Operator i infrastrukturës së rëndësishme të informacionit" (OIRI) është një person juridik publik, që administron infrastrukturë të rëndësishme të informacionit.

Masat e sigurisë grupohen në dy nivele, si më poshtë:

Përshkrimi i niveleve të sigurisë
Niveli i parë (Masat që janë të detyrueshme për OIRI dhe OIKI) • Masa sigurie bazike që duhen implementuar për të arritur objektivat e sigurisë • Evidenca që masat bazike të sigurisë janë implementuar • Masat e sigurisë të nivelit mesatar për të arritur objektivin dhe një rishikim ad-hoc të zbatimit, pas ndryshimeve apo incidenteve. • Dëshmia e masave të sigurisë së nivelit mesatar dhe evidencat e rishikimeve të zbatimit pas ndryshimeve ose incidenteve.
Niveli i dytë (Masat që janë të detyrueshme për OIKI) • Masa sigurie në nivel të avancuar 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. • Evidenca e zbatimit të avancuar të masave të sigurisë, evidencat e një procesi të shqyrtimit strukturor dhe evidenca të hapave pro - aktiv për të përmirësuar zbatimin e masave të sigurisë.

Shënim: 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 organizative janë ato të:

a) menaxhimit të sigurisë së informacionit,
b) menaxhimit të rrezikut,
c) politikave të sigurisë,
ç) sigurisë organizative,
d) kërkesave të sigurisë për palët e treta,
dh) menaxhimit të aseteve,
e) sigurisë së burimeve njerëzore dhe aksesit të personave,
ë) ngjarjeve të sigurisë dhe menaxhimit të incidenteve të sigurisë kibernetike,
f) menaxhimit të vazhdimësisë së punës,
g) kontrollit dhe auditit,

a) Menaxhimi i sigurisë së informacionit

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të sigurohet pajtueshmëri me ligjet aktuale, rregullore dhe udhëzime.	• Udhëzimi i bazave të të dhënave shtetërore
	b) Të sigurohet pajtueshmëri në përputhje me kërkesat e konfidencialitetit, integritetit dhe disponueshmërisë për punonjësit e institucionit dhe përdoruesit e tjerë.	• Politikat e Sigurisë së Informacionit • Objektivat dhe Planifikimi i Sigurisë së Informacionit. • Dokumentimi i Menaxhimit të roleve dhe Përgjegjësive.
	c) Të vendosen kontrolle për mbrojtjen e informacionit të institucionit dhe sistemet e informacionit kundër vjedhjes, abuzimit dhe format e tjera të dëmit dhe humbjes. d) Të jenë të ndërgjegjshëm për sigurinë e informacionit administratorët dhe punonjësit, në mënyrë që të minimizohet rreziku i incidenteve të sigurisë.	• Dokumentim i kontrolleve për mbrojtjen e informacionit në përputhje me metodat nga standardet ndërkombëtare për sigurinë e informacionit, p.sh. ISO / IEC 27001.
2	e) Të sigurohet që institucioni të jetë i aftë për të vazhduar shërbimet e tij edhe në qoftë se ndodhin incidente të sigurisë.	• Dokumentimi implementimit të Dis recovery • Plan i trajtimit të rrezikut. • Procedurë e trajtimit të rrezikut • Mjet (tool) për vlerësimin e rrezikut. • Inventarizim dhe pronësim të aseteve SW&HW, si dhe të sistemeve. • Dokumenti i sigurisë fizike dhe ambient ale. • Plani dhe Planifikimi i vazhdimësisë për Sigurinë e Informacionit. • Dokumenti i testimit të Sigurisë së Vazhdimësisë.
	f) Të sigurohet mbrojtja e të dhënave personale (privatësisë).	• Dokumentim për mbrojtjen e të dhënave personale

b) Menaxhimi i rrezikut

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të bëhet një listë e rreziqeve kryesore për sigurinë dhe vazhdimësinë e sistemeve të informacionit dhe rrjeteve, duke marrë në konsideratë kërcënimet kryesore për burimet e rëndësishme. b) Të vendoset në dijeni personeli i autorizuar për rreziqet kryesore dhe për mënyrën se si ti trajtojë ato.	◦ Listë e rreziqeve kryesore të përshkruara në një nivel të lartë, duke përfshirë rreziqet themelore dhe impaktin e tyre potencial në sigurinë dhe vazhdimësinë e sistemeve të informacionit dhe rrjeteve të komunikimit. ◦ Dokumentim i njohjes së personelit me rreziqet kryesore.
	c) Të krijohet dhe të vendoset një metodologji e menaxhimit të rrezikut dhe / ose mjetet bazuar në standardet e sigurisë. d) Të sigurohet që personeli kryesor përdor metodologjinë dhe mjetet e menaxhimit të rrezikut. e) Të rishikohen vlerësimet e rrezikut pas ndryshimeve ose incidenteve. f) Të sigurohet që disa prej rreziqeve janë pranuar nga menaxhimi.	◦ Metodologjia dhe / ose mjetet e menaxhimit të rrezikut të dokumentuara. ◦ Udhëzimi për personelin në vlerësimin e rreziqeve. ◦ Listë e rreziqeve dhe evidencat e rishikimeve / përditësimeve. ◦ Të dokumentohet rishikimi i vlerësimeve të rreziqeve ◦ Të dokumentohet miratimi i menaxhimit për rreziqet e pranuara.
2	g) Të rishikohet metodologjia dhe / ose mjetet e menaxhimit të rrezikut, në mënyrë periodike, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	◦ Dokumentim i procesit të rishikimit dhe përditësimeve të metodologjisë dhe / ose mjeteve të menaxhimit të rrezikut.

c) Politikat e sigurisë

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të vendoset një politikë sigurie e nivelit të lartë që adreson sigurinë dhe vazhdimësinë e sistemeve të informacionit dhe rrjeteve të komunikimit dhe / ose shërbimeve të ofruara prej tyre.	• Të dokumentohet vënia në dijeni e personelit të autorizuar mbi politikën e sigurisë dhe objektivat të saj. • Të dokumentohen politikat e sigurisë së informacionit të aprovuara nga stafi menaxhues, duke përfshirë ligjin dhe rregulloret e zbatueshme.
	b) Të implementohen politika të detajuara të sigurisë së informacionit për burimet kritike. c) Të vihet në dijeni i gjithë personeli për politikën e sigurisë dhe për çfarë lidhet me punën e tyre. d) Të rishikohet politika e sigurisë pas incidenteve në qoftë se konsiderohet e nevojshme.	• Të rishikohen komentet ose të ndryshohen pjesë të politikës dhe të dokumentohen. • Dokumenti i roleve dhe përgjegjësive të Menaxhimit të dokumentacioneve. • Plani i menaxhimit të sistemeve të sigurisë së informacionit. • Kuadri / struktura e menaxhimit të rrezikut. • Deklarata e Zbatimit të Udhëzimeve të Punës. • Plani i trajtimeve të rrezikut. • Kërkesat e shqyrtimit të personelit. • Inventari i menaxhimit të Aseteve.
2	e) Të rishikohet politika e sigurisë së informacionit në mënyrë periodike dhe të merren në konsideratë shkeljet, përjashtimet, incidentet e mëparshme, testet / ushtrimet e mëparshme.	• Të dokumentohen politikat e sigurisë së informacionit të aprovuara nga stafi menaxhues • Të dokumentohet procesi i rishikimit, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.

ç) Siguria Organizative

Niveli i sigurisë	Masat	Dokumentimi
1	a) T'u caktohen punonjësve rolet e sigurisë dhe përgjegjësitë. b) Të sigurohet që rolet e sigurisë janë të menaxhueshme në rast se ndodhin incidente sigurie.	• Listë e roleve të sigurisë dhe informacione kontakti. • Plani i Sistemit te Menaxhimit të Sigurisë së Informacionit. • Objektivat e sigurisë së informacionit • Kërkesat e burimeve njerëzore për marrjen në punë të personelit. • Kërkesat e verifikimit të sigurisë së personelit. • Dokumenti i përfundimit të marrëdhënieve të punës. • Dokumenti i menaxhimit dhe aksesit të përdoruesve
	c) T'u caktohen punonjës-ve në mënyrë zyrtare rolet e sigurisë. d) Të vihen në dijeni punonjësit për rolet e sigurisë në institucion si edhe kur duhet të kontaktohen	• Dokumenti i sigurisë dhe përdorimit të pajisjeve teknologjike. • Dokumenti i sigurisë fizike. • Listë e emërimeve dhe përshkrimi i përgjegjësive dhe detyrave për rolet e sigurisë. • Materiale ndërgjegjësimi dhe informimi për punonjësin duke shpjeguar rolet e sigurisë dhe si / ku ata duhet të kontaktohen.
2	e) Struktura e roleve të sigurisë dhe përgjegjësive rishikohet rregullisht, si pasojë e ndryshimeve dhe / ose incidenteve të mëparshme.	• Dokumentim i përditësuar i strukturës së detyrave të roleve të sigurisë dhe përgjegjësive. • Dokumentim i procesit të rishikimit, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.

d) Kërkesat e sigurisë për palët e treta

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të vendoset një politikë sigurie për kontratat me palët e treta. b) Të sigurohet që të gjitha prokurimet e shërbimeve / produkteve nga palët e treta janë në përputhje me politikën.	• Dokumenti i saktësimit dhe përcaktimit të palëve të treta. • Dokumenti shabllon i një kontrate me palët te treta. • Dokumenti i politikave të sigurisë së informacionit për marrëdhëniet me palët e treta. • Dokumentim i kërkesa të qarta të sigurisë në kontratat me palët e treta që na furnizojnë me produkte IT, shërbime IT, procese biznesi outsource, helpdesks, call center, pajisje të përbashkëta, etj.
	c) Të rishikohen politikat e sigurisë për palët e treta, pas incidenteve ose ndryshimeve në qoftë se konsiderohet e nevojshme.	• Politikë sigurie e dokumentuar për kontratat me palët e treta. • Listë e kontratave me palët e treta. Kontratat për shërbime me palë të treta përmbajnë kërkesa sigurie në përputhje me politikën e sigurisë për prokurimet. • Të dokumentohet rishikimi i komenteve ose ndryshimet e politikës.
	d) Të reduktohen rreziqet e mbetura që nuk janë të adresuara nga pala e tretë.	• Listë e rreziqeve të pranuara që trajtohen me palët e treta.
2	e) Të mbahen rekorde të incidenteve të sigurisë të lidhura ose të shkaktuara nga palët e treta. f) Të rishikohen dhe të përditësohen politikat e sigurisë për palët e treta në intervale të rregullta, duke marrë në konsideratë incidentet dhe ndryshimet e mëparshme.	• Listë e incidenteve të sigurisë të lidhura ose të shkaktuara nga angazhimi me palët e treta • Dokumentim i procesit të rishikimit të politikës.

dh) Menaxhimi i aseteve

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të menaxhohen burimet kritike dhe të konfigurohen sistemet kritike. b) Të implementohen politikat / procedurat për menaxhimin e burimeve dhe kontrollin e konfigurimit.	◦ Dokumenti i inventarizimit dhe pronësisë së aseteve ◦ Dokumenti i politikave të përdorimit të internetit të sigurt. ◦ Dokumenti i rregullave për përdorimin e emal-it ◦ Dokumenti i rregullave të përdorimit të pajisjeve periferike të përbashkëta si fotokopje, fax etj. ◦ Dokumenti i klasifikimit të sigurisë së informacionit. ◦ Dokumenti i trajtimit të informacionit. ◦ Dokumenti i marrjes në dorëzim dhe shkatërrimit të aseteve. ◦ Lista e burimet dhe sistemeve kritike. ◦ Politikat e dokumentuara / procedurat për menaxhimin e aseteve, duke përfshirë rregullat dhe përgjegjësitë e burimeve dhe konfigurimet të cilat janë subjekt i politikave.
2	c) Të rishikohen dhe përditësohen herë pas here politikat e menaxhimit të burimeve, bazuar në ndryshimet dhe incidentet e shkuara.	◦ Një inventar burimesh ose inventarë, të cilët përmbajnë burime kritike dhe varësinë ndërmjet aseteve. ◦ Të dokumentohet përditësimi i politikave të menaxhimit.

e) Siguria e burimeve njerëzore dhe aksesit të personave

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të kontrollohen referencat profesionale të personelit (administratorit të sistemit, oficerëve të sigurisë, etj.)	◦ Dokumenti i politikave të kontrollit te aksesit. ◦ Dokumenti i menaxhimit të aksesit të përdoruesve. ◦ Dokumenti i menaxhimit të username dhe fjalëkalimeve. ◦ Shtojca e përdorimit të wireless. ◦ Shtojca e përdorimit të telefonave celular. ◦ Dokumenti për përdorimin e shërbimeve të sistemit. ◦ Kërkesa për fshirjen e përdoruesit. ◦ Kërkesa për zëvendësimin e përdoruesit. ◦ Dokumenti i aksesit të sistemit nga jashtë perimetrit. ◦ Dokumenti i sigurisë fizike dhe ambientale. ◦ Dokumenti i monitorimit të alarmeve (dyer emergjence, zjarr, vjedhje) ◦ Dokumenti i sigurisë së pajisjeve. ◦ Dokumenti i sigurisë së perimetrit. ◦ Dokumenti i sigurisë për personat e jashtëm jo personel. ◦ Dokumenti i kontrollit të referencave profesionale për personelin.
	b) Të vendoset një politikë dhe procedurë për kontrollet e background-it. c) Të kryhen verifikime të background-it për personelin kyç, kur nevojitet dhe lejohet ligjërisht.	◦ Politikë dhe procedurë për kontrollet e background-it. ◦ Udhëzim për personelin se kur / si të kryej kontrolle të background-it.
2	d) Të rishikohen dhe përditësohen politikat / procedurat për kontrollet e background-it dhe referencës në mënyrë periodike, duke marrës në konsideratë ndryshimet dhe incidentet e mëparshme.	◦ Dokumentim i rishikimit të komenteve ose ndryshimeve të politikës / procedurës.

e) Ngjarjet e sigurisë dhe menaxhimit të incidenteve të sigurisë kibernetike

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të sigurohet që personeli është në gatishmëri dhe i përgatitur të menaxhojë dhe ti përballojë incidentet.	◦ Raportet e dobësive dhe ngjarjeve të sigurisë se informacionit. ◦ Dokumenti i përgjigjeve të raporteve të sigurisë së informacionit. ◦ Dokumenti mbledhjes së provave / evidencave. ◦ Raport i ngjarjes të sigurisë së informacionit.
	b) Të regjistrohen incidentet kryesore. c) Të implementohen politikat / procedurat për menaxhimin e incidenteve.	◦ Inventarizimi i incidenteve kryesore dhe për incidentet, impaktin, shkakun veprimet e ndërmarra, dhe mësimin e nxjerrë. ◦ Dokumenti / procedurat për menaxhimin e incidenteve, duke përfshire llojin e incidentit që mund të ndodhë, objektivat, rolin dhe përgjegjësitë, përshkrim i detajuar, për tipin e incidentit, si ta menaxhojmë incidentin, si të shkallëzojmë tek menaxheri etj.
2	d) Të investigohen incidentet kryesore dhe raportimi i tyre final, duke përfshire veprime të ndërmarra dhe rekomandime për të zvogëluar incidente të ngjashme. e) Të vlerësohen politikat e menaxhimit të incidenteve / procedurave bazuar në incidente të shkuara	◦ Raporte individuale i përballimit të shumicës së incidenteve. ◦ Politika të përditësuara të menaxhimit / procedurave rishikim komentesh dhe / ose ndryshim i logs.

f) Menaxhimi i vazhdimësisë së punës

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të implementohet një strategji për vazhdimësinë e shërbimit për rrjetet e komunikimeve dhe / ose shërbimeve të ofruara.	◦ Dokumenti i planifikimit të Vazhdimësisë së Sigurisë së Informacionit ◦ Plani i Vazhdimësisë së Sigurisë së Informacionit. ◦ Vlerësimi i Riskut të Sigurisë së Informacionit. ◦ Testimi i Vazhdimësisë së Sigurisë së Informacionit. ◦ Strategji e dokumentuar për vazhdimësinë e shërbimit, duke përfshirë objektivat kohë për shërbimet kryesore dhe proceseve.
	b) Të zbatohen plane rezervë për sistemet kritike. c) Të aktivizohet monitorimi dhe zbatimi i planeve të paparashikuara, të regjistrohen tentativat e suksesshme dhe të kohës së dështimit.	◦ Plane emergjence për sistemet kritike,duke përfshirë hapa të qarta dhe procedurat për kërcënimet e njohura, shkaktuesit për aktivizimin, hapat dhe objektivat kohore. ◦ Dokumentim i planeve emergjente, duke përfshirë vendimet e marra dhe hapat e ndjekur.
2	d) Të rishikohen shërbimet strategjike në mënyrë të vazhdueshme dhe periodikisht. e) Të rishikohen planet e emergjencave, bazuar në incidentet e fundit dhe ndryshimet. f) Të përgatiten për rikthimin në gjendje normale të shërbimeve në katastrofën potenciale të radhës. g) Të vendoset një mekanizëm për normalizimin e situatës. h) Të kontrollohen dhe përditësohen kapacitetet në mënyre të vazhdueshme të rregullt, duke marrë parasysh ndryshimet që ndodhin, incidentet e mëparshme, rezultatet e testeve.	◦ Përditësimi i strategjisë në vazhdueshmëri dhe planin e incidenteve, rishikim komentesh, dhe / ose ndryshim i logs. ◦ Procedurat / politika të dokumentuara / për efektivitetin sa më të lartë të kapaciteteve për rimëkëmbjen e situatës, duke përfshirë një listë të katastrofave natyrale që mund ndikojnë në shërbime, dhe nja listë të kapaciteteve (ato nga palët e treta por edhe ato të brendshëm). ◦ Dokumentim i të gjithë mekanizmave failover parandalues për katastrofat natyrale me pasoja të mëdha. ◦ Dokumentimi i kapaciteteve për rregullimin e situatës në fjale , të shikohen komentet dhe / ose ndryshim i logs.

g)Kontrolli dhe auditi

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të implementohet monitorimi i logeve për sistemet e informacionit. b) Të implementohet politika e ngjarjeve dhe monitori-min e sistemeve. c) Të vendosen mjete për monitorimin e sistemeve të informacionit. d) Të vendosen mjetet për të mbledhur dhe ruajtur shkrimet e sistemeve të informacionit.	‘ Procedura e vlerësimit të performancës ‘ Procedura e audit të brendshëm. ‘ Rishikimi menaxherial të menaxhimit të sigurisë të sistemeve të informacionit. ‘ Raport i auditive të brendshëm. ‘ Raport i rishikimeve menaxheriale. ‘ Loget dhe raportet e monitorimit të rrjetit të komunikimit dhe të sistemeve te informacionit. ‘ Politika të dokumentuara për monitorimin dhe ngjarjet, duke përfshirë kërkesat minimale për monitorimin dhe ngjarjet, periudhën e mbajtjes, dhe objektivat e përgjithshme të ruajtjes.
2	e) Të rishikohet dhe përditësohet monitorimi i politikave / procedurave, duke marrë parasysh ndryshimet dhe incidentet e shkuara.	‘ Dokumentacioni i monitorimit dhe politikat e ngjarjeve / procedurat, të dokumentuara.

Masat teknike janë ato të:

a) sigurisë fizike,

b) mbrojtjes së integritetit të rrjeteve të komunikimit,

c) verifikimit të identitetit të përdoruesve,

ç) menaxhimit për autorizimin e aksesit,

d) veprimtarisë së administratorëve dhe të përdoruesve,

dh) zbulimit të ngjarjeve të sigurisë kibernetike,

e) mjeteve të gjurmimit dhe vlerësimit të ngjarjeve të sigurisë kibernetike,

ë) sigurisë së aplikacioneve,

f) të pajisjeve kriptografike,

g) sigurisë së sistemeve industriale.

a) Siguria Fizike

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të eliminohet aksesi fizik i paautorizuar tek pajisjet dhe infrastruktura dhe të kryhen kontrolle mjedisore për mbrojtjen ndaj hyrjes së paautorizuar, vjedhjes, zjarrit, përmbytjeve etj. b) Të eliminohet aksesi fizik i paautorizuar të pajisjet dhe infrastruktura dhe të kryhen kontrolle mjedisore për mbrojtjen ndaj hyrjes së paautorizuar, vjedhjes, zjarrit, përmbytjeve etj. c) Të implementohet një politikë për masat e sigurisë fizike dhe kontrolleve të mjedisit.	▪ Të dokumentohet implementimi bazë i masave të sigurisë fizike dhe kontrolleve mjedisore, si çelësa, alarm ndaj vjedhjes, zjarrit, dhe sistemin për shuarjen e tij etj. ▪ Politikë e dokumentuar për masat e sigurisë fizike dhe kontrolleve të mjedisit, duke përfshirë përshkrimin e pajisjeve dhe sistemeve. ▪ Të dokumentohen kontrollet fizike të mjedisit, si kontrollin elektronik të hyrjes dhe mjete të gjurmimit, ndarje të hapësirave sipas niveleve të autorizimit, fikëse automatike zjarri etj.
2	d) Të vlerësohet efektiviteti i kontrolleve fizike dhe mjedisit periodikisht. e) Të rishikohen dhe përditësohen politikat për masat e sigurisë fizike dhe kontrollet e mjedisit duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	▪ Politikë e përditësuar për masat e sigurisë fizike dhe kontrollet e mjedisit. ▪ Dokumentim i vlerësimit të kontrollit mjedisor, të rishikohen komentet ose ndryshimet.

b) Mbrojtja e integritetit të rrjeteve të komunikimit

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të sigurohet që programet e rrjetit të komunikimit dhe sistemet e informacionit nuk janë deformuar ose ndryshuar, duke përdorur kontrollin e inputeve dhe firewall-et. b) Të sigurohet që të dhënat kritike të sigurisë si password -et, çelësat privatë, nuk bëhen publike.	• Dokumenti për mbrojtjen e programeve dhe të dhënave në rrjet dhe sistemeve të informacionit nëpërmjet kontrollit të inputeve, firewall-et, enkriptimi dhe nënshkrimi. • Dokumentimi i mbrojtjes së të dhënave me mekanizma të mbrojtjes si memorie të shpërndarë, enkriptimi
	c) Të kontrollohet për programe të dëmshme në rrjetet e komunikimit dhe sistemet e informacionit. d) Të implementohen masa sigurie sipas standardeve, duke ofruar mbrojtje ndaj modifikimit të sistemeve.	• Të dokumentohet ekzistenca dhe përditësimi i sistemeve të zbulimit të programeve të dëmshme • Dokumentim i mbrojtjes dhe implementimit të programeve dhe të dhënave në rrjet dhe në sistemet e informacionit. • Mjete për zbulimin e përdorimit jonormal të sistemeve ose sjelljeve jonormale të sistemeve (si sistemet e zbulimit të ndërhyrjeve dhe anomalive). • Loge të sistemeve të zbulimit të ndërhyrjeve dhe anomalive
2	e) Të vendosen kontrolle të mbrojtjes së integritetit të sistemeve. f) Të vlerësohen dhe rishikohen efektiviteti i masave për të mbrojtur integritetin e sistemeve.	• Dokumentim i kontrolleve të përditësuara për të mbrojtur integritetin e sistemeve. • Dokumentim i procesit të kontrollit të logeve për sistemet e zbulimit të ndërhyrjeve dhe anomalive.

c) Verifikimi i identitetit të përdoruesve

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të imlementohet monitorimi i të dhënave kritike. b) Të implementohet politika e ngjarjeve dhe monitorimi i sistemeve kritike. c) Të vendosen mjete për monitorimin e sistemeve kritike.	◦ Raportet e monitorimit të rrjetit kritik dhe të sistemeve te informacionit ◦ Kërkesat për verifikimin e figurës së përdoruesve. ◦ Dokumenti i kërkesave për akses.
2	d) Të vendosen mjetet për të mbledhur dhe ruajtur shkrimet e të dhënave kritike	◦ Politika të dokumentuara për monitorimin dhe ngjarjet, duke përfshirë kërkesat minimale për monitorimin dhe ngjarjet, periudhën e mbajtjes, objektivat e përgjithshme të ruajtjes, monitorimin e të dhënave dhe log-et.

ç) Menaxhimit për autorizimin e aksesit

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të implementohet mekanizmi i duhur i kontrollit logjik për rrjetin dhe sistemet e informacionit për të lejuar vetëm kontrollin e autorizuar. b) Të implementohen politika për mbrojtjen e aksesit në rrjet dhe sistemet e informacionit, duke adresuar rolet, të drejtat, përgjegjësitë dhe procedurat për vendosjen dhe revokimin e të drejtave të aksesit. c) Të zgjidhen mekanizmat e duhur të autentikimit në varësi të tipit të aksesit.	▪ Përmbledhje e autentikimit dhe metodave të kontrollit të aksesit për sistemet dhe përdoruesit. ▪ Marrëveshje individuale për akses. ▪ Dokumenti i aksesit të pajisjeve periferike (fotokopje, fax etj.) ▪ Politikë e kontrollit të aksesit duke përfshirë përshkrimin e roleve, grupeve, të drejtave të aksesit, procedurat për dhënien dhe revokimin e aksesit. Dokumenti i menaxhimit të media dhe mirëmbajtjes së informacionit. ▪ Politika e përdorimit të internetit.
2	d) Të monitorohet aksesi në rrjet dhe sistemet e informacionit, të vendoset një proces i miratimit të përjashtimeve dhe regjistrimit të thyerjeve të aksesit.	▪ Dokumentim i monitorimit të aksesit në rrjet dhe sistemeve të informacionit.

d)Veprimtaria e administratorëve dhe e përdoruesve

Niveli i sigurisë	Masat	Dokumentimi
1	a) T'i caktohen personelit rolet e sigurisë dhe përgjegjësitë. b) Të sigurohet që rolet e sigurisë janë të arritshme në rast se ndodhin incidente sigurie c) Të emërohet personeli zyrtarisht në rolet e sigurisë. d) Të vendoset personeli në dijeni të roleve të sigurisë në organizatë dhe kur duhet të kontaktohen.	◦ Listë e emërimeve (CISO, DPO,etj.) dhe përshkrimi i përgjegjësive dhe detyrave për rolet e sigurisë(CISO, DPO, etj. ◦ Materiale ndërgjegjësimi dhe informimi për personelin duke shpjeguar rolet e sigurisë dhe kur / si ata duhet të kontaktohen. ◦ Listë e pozicioneve të sigurisë (menaxher i vazhdimësisë së biznesit, etj.)
2	e) Të rishikohet rregullisht struktura e roleve të sigurisë dhe përgjegjësive, si pasojë e ndryshimeve dhe / ose incidenteve të mëparshme.	◦ Dokumentim i procesit të rishikimit, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme

dh) Zbulimi i ngjarjeve të sigurisë kibernetike

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të ngrihen kapacitetet e proceseve apo sistemeve për zbulimin e ngjarjeve të sigurisë kibernetike. b) Të implementohen sistemet dhe procedurat për zbulimin e ngjarjeve të sigurisë kibernetike. c) Të implementohen sistemet dhe procedurat për regjistrimin dhe përcjelljen e incidenteve në kohë të njerëzit e duhur.	▪ Të dokumentohet ngritja e kapaciteteve të proceseve apo sistemeve. ▪ Dokumentim i sistemeve dhe procedurave të zbulimit te ngjarjeve, të tilla programe për informacionin e Sigurisë për Menaxhimin e Ngjarjeve (SIEM) .
2	d) Të rishikohen sistemet dhe proceset për zbulimin e ngjarjeve rregullisht dhe përditësimin e tyre duke marrë parasysh ndryshimet dhe incidentet e fundit.	▪ Përditësimi i dokumentacionit të sistemeve të zbulimit incidenteve dhe proceseve. ▪ Dokumentimi i rishikimit të procesit të zbulimit të incidentit, shqyrtimi i komenteve, dhe / ose ndryshim i logeve.

e) Mjetet e gjurmimit dhe vlerësimit të ngjarjeve të sigurisë kibernetike

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të përcaktohen rregullat e përgjithshme që duhet të jenë të qarta për çdo punonjës / përgjegjës për menaxhimin e log-eve të administratës publike. Institucionet shtetërore janë përgjegjëse për informacionin që ato trajtojnë.	• Një rregullore e shkruar për menaxhimin e log-eve sipas kërkesave të institucionit. Log-et duhet të ruhen në ambiente të cilat kanë sigurinë e nevojshme fizike dhe janë të mbrojtura nga lagështira, fushat magnetike, zjarri etj.
2	b) Të aplikohen një sërë rregullash dhe procedurash për ruajtjen e integritetit dhe konfidencialitetit të informacionit.	• Log-et për çdo veprim të kryer në sistemet e institucionit duhet të ruhen minimalisht sipas afateve të përcaktuara.

ë) Siguria e aplikacioneve

Niveli i sigurisë	Masat	Dokumentimi
1	a) Të kryhen vlerësimet e sigurisë e aplikimit web nga personeli i sigurimit të deleguara ose të punësuar ose të kontraktuar nga institucioni. Të gjitha gjetjet që janë konsideruar konfidenciale, duhet të shpërndahen personave me një " nevojë për njohje " bazë. Shpërndarja gjetjeve jashtë institucionit është rreptësishtë e ndaluar, përveç nëse miratohet nga eprori.	◦ Dokumenti i vlerësimeve të sigurisë.
2	b) Çdo marrëdhënie brenda aplikacioneve do të përfshihen në vlerësimin nëse nuk kufizohet në mënyrë eksplicite.	◦ Dokumenti i vlerësimeve të sigurisë.

f) Të pajisjeve kriptografike

Niveli i sigurisë	Masat	Dokumentimi
1	a) Kriptografi bazuar në rrjet Sistemet kriptografike bazuar në problemet kriptografisë me bazë rrjetë kanë rimarrë interes, për disa arsye. Aplikacionet e reja kanë bërë të mundur përdorimin e kriptografisë me bazë rrjetë. Shumica e pajisjeve të kriptografisë me bazë rrjeti janë të thjeshta dhe efikase. Gjithashtu, siguria e disa sistemeve me bazë rrjeti është e sigurtë. b) Kriptografi bazuar në kod – Sistemi kripto McEliece u propozua për herë të parë në 1978, dhe ka nuk është thyer që nga ai vit. Që nga ajo kohë, sisteme të tjera të bazuara në kodet korrigjim gabimi- janë propozuar, pavarësisht se ka një kod me madhësi të madhe. Në versionet e reja është paraqitur një kod me madhësi më të zvogëluar, gjithsesi dhe struktura e re ka rezultuar me sukses. Kriptografia e bazuar në kod ka rezultuar më e suksesshme se kriptografia bazuar në nënshkrim.	✓ Dokumenti i politikave te enkriptimit. ✓ Dokumenti i menaxhimit të çelësave kriptografik. ✓ Dokumenti i kontrolleve të sigurisë kriptografike. ✓ Raporti i kontrolleve pajisjeve kriptografike. ✓ Duhet të bëhen parashikimet për koston e prishjes së këtyre crypto sistemeve. Për sistemet simetrike kryesore, një orientues i thjeshtë është që të dyfishohet gjatësia e çelësit.
2	c) Nënshkrimet me bazë hash - Nënshkrimet me bazë hash janë nënshkrime digjitale të ndërtuara duke përdorur funksione hash. Siguria e tyre, madje edhe nga sulmet kuantike, është kuptuar mirë. Skemat efikase të nënshkrimit me bazë hash duhet të përmbajnë një regjistër me numrin e saktë i mesazheve të nënshkruara më parë, dhe çdo gabim në këtë arkiv të dhënash do të rezultojë në pasiguri. Numri i nënshkrimeve mund të rritet, madje edhe deri në pikën e të qenit në mënyrë efektive të pakufizuar, por kjo gjithashtu rrit madhësinë e nënshkrimit.	✓ Zhvillimi i standardeve për kriptografinë do të kërkojnë burime të konsiderueshme për të analizuar skemat, dhe do të kërkojë angazhim të rëndësishëm publik. ✓ Duhet të planifikohen kriteret vlerësimit të standardeve kryesore kriptografisë.

g) Siguria e sistemeve industriale

Niveli i sigurisë	Masat	Dokumentimi
2	a) Kontrolli i sistemeve industriale, duke përfshirë kontrollin mbikëqyrjes së të dhënave, kontrollin e sistemeve, dhe konfigurime të tjera të sistemit të kontrollit të tilla si kontrollin e programeve logjike. b) Trajtimin e performancës unike, besueshmërinë dhe sigurisë së kërkesave.	• Përditësim të Kontrollit të sistemeve industriale, kërcënimet dhe dobësitë. • Përditësim për menaxhimin e rrezikut në sistemet industriale, praktikat e rekomanduara dhe arkitektura. • Përditësim për aktivitetet aktuale në sigurinë e sistemeve industriale. • Përditësim për aftësitë e sigurisë dhe mjetet për sistemet industriale. shtrirjes shtesë me standardet e tjera të sigurisë dhe udhëzimet. • Standarde dhe udhëzime të reja për sistemet industriale • Zhvillimin e politikave të sigurisë, procedurat, trajnimin dhe materiale edukative që vlen në mënyrë specifike për SI. • Duke marrë parasysh politikat e sigurisë për sistemet industriale dhe procedurat bazuar në nivelin e kërcënimit. • Duke iu drejtuar sigurisë gjatë gjithë ciklit të jetës së sistemeve industriale nga dizajni i arkitekturës të prokurimit të instalimit tek mirëmbajtja e sistemit. • Zbatimi i një topologjie rrjeti për sistemet industriale që ka shtresa të shumëfishta, me komunikimet më kritike ndodhen në shtresën më të sigurtë dhe të besueshme. • Projektimi sistemeve kritike për degradim (pjesë e tolerancës) për të parandaluar ngjarjet katastrofike. • Paaftësi portet dhe shërbime në pajisjet SHKB papërdorura pas testimit për të siguruar se kjo nuk do të ndikojë operacion ICS. • Kufizimi në akses fizik në rrjetin dhe pajisjet e sistemeve industriale • Kufizimi i drejtave të përdoruesit vetëm ata që janë të nevojshëm për të kryer punën (d.m.th., duke vendosur kontrollin e aksesit të bazuar në konfigurimin për çdo rol kyç)në sistemet industriale • Përdorimi i mekanizmave të veçanta të autentifikimit dhe kredencialet për përdoruesit e rrjetit në sistemet industriale dhe rrjetit të korporatës (d.m.th., llogaritë e rrjetit sistemet industriale nuk i përdorin llogaritë e përdoruesve të rrjetit të korporatës)