



www.qbz.gov.al

FLETORJA ZYRTARE E REPUBLIKËS SË SHQIPËRISË

Botim i Qendrës së Botimeve Zyrtare

Viti: 2015 – Numri: 212

Tiranë – E premte, 11 dhjetor 2015

PËRMBAJTJA

	Faqe
Vendim i Këshillit të Ministrave nr. 969, datë 2.12.2015	Për miratimin e rregullores “Për kërkesat minimale për mbrojtjen e sigurisë e të shëndetit të punëmarrësve në industritë minerare nxjerrëse, sipërfaqësore dhe nëntokësore”..... 13981
Vendim i Këshillit të Ministrave nr. 973, datë 2.12.2015	Për miratimin e dokumentit të politikave për sigurinë kibernetike 2015–2017..... 13995



VENDIM
Nr. 969, datë 2.12.2015

PËR MIRATIMIN E RREGULLORES
“PËR KËRKESAT MINIMALE PËR
MBROJTJEN E SIGURISË E TË
SHËNDETIT TË PUNËMARRËSVE NË
INDUSTRI TË MINERARE NXJERRËSE,
SIPËRFAQËSORE DHE
NËNTOKËSORE”

Në bazë të nenit 100 të Kushtetutës, të pikës 3, të nenit 42, të ligjit nr. 10237, datë 18.2.2010, “Për sigurinë dhe shëndetin në punë”, të ndryshuar, dhe të pikës 2, të nenit 3, të ligjit nr. 8741, datë 15.2.2001, “Për sigurinë në punë në veprimtarinë minerare”, të ndryshuar, me propozimin e ministrit të Energjisë dhe Industrisë, Këshilli i Ministrave

VENDOSI:

1. Miratimin e rregullore “Për kërkesat minimale për mbrojtjen e sigurisë e të shëndetit të punëmarrësve në industritë minerare nxjerrëse, sipërfaqësore dhe nëntokësore¹”, sipas tekstit bashkëlidhur këtij vendimi.

2. Ngarkohet Ministria e Energjisë dhe Industrisë për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare dhe i shtrin efektet e tij 6 muaj pas botimit.

KRYEMINISTRI
Edi Rama

RREGULLORE
PËR KËRKESAT MINIMALE PËR
MBROJTJEN E SIGURISË E TË SHËNDETIT
TË PUNËMARRËSVE NË INDUSTRI TË
MINERARE NXJERRËSE, SIPËRFAQËSORE
DHE NËNTOKËSORE

SEKSIONI I
DISPOZITA TË PËRGJITHSHME

¹ Kjo rregullore transponon direktivën e Këshillit 92/104/KEE mbi kërkesat minimum për përmirësimin e mbrojtjes së sigurisë dhe shëndetit të punonjësve në industritë minerare-nxjerrëse, sipërfaqësore dhe nëntokësore (direktiva e 12 individuale në kuptim të nenit 16 (1) të direktivës 89/391/KEE. Kjo rregullore përcakton detyrimet e përgjithshme të punëdhënësit, kërkesat e përgjithshme për sigurimin e informacionit, udhëzimit dhe formimit, dhe përdorimin e metodave të sigurta të punës, si dhe kërkesa specifike të zbatueshme për industritë minerare-nxjerrëse, sipërfaqësore dhe nëntokësore.

Neni 1
Objekti

1. Kjo rregullore përcakton kërkesat minimale për mbrojtjen e punëmarrësve në industritë minerare-nxjerrëse, sipërfaqësore dhe nëntokësore, nga risqet për sigurinë dhe shëndetin në punë dhe është e zbatueshme për të gjithë punëdhënësit që kryejnë veprimtari në këtë fushë.

2. Dispozitat e ligjit nr. 10237, datë 18.2.2010, “Për sigurinë dhe shëndetin në punë”, dhe të ligjit nr. 8741, datë 15.2.2001, “Për sigurinë në punë në veprimtarinë minerare”, zbatohen plotësisht pa cenuar dispozitat më shtrënguese dhe/ose specifike të ndodhura në këtë rregullore.

Neni 2
Përkufizime

Për efekt të kësaj rregulloreje, me termat e mëposhtëm nënkuptohet:

1. “Industri nxjerrëse nëntokësore”, çdo industri që praktikon çdonjërin prej aktiviteteve të mëposhtme:

a) Nxjerrjen nëntokësore të mineraleve;

b) Kërkimin me synimin për të kryer këtë lloj nxjerrjeje, ku përfshihen instalime ndihmëse sipërfaqësore;

c) Përgatitjen e çdolloj materiali të tillë, të nxjerrë në këtë mënyrë për shitje, me përjashtim të veprimtarive të çfarëdolloj procesi të prodhimit të këtyre materialeve, duke përjashtuar industritë e nxjerrjes së materialeve nëpërmjet shpimit të përcaktuara në nenin 2 të rregullore për “Për kërkesat minimale për mbrojtjen e sigurisë dhe shëndetit të punëmarrësve në industritë minerare nxjerrëse nëpërmjet shpimit”.

2. “Industri nxjerrëse sipërfaqësore”, çdo industri që praktikon çdonjërin prej aktiviteteve të mëposhtme:

a) Nxjerrjen sipërfaqësore të mineraleve;

b) Kërkimin dhe zbulimin me synimin për të kryer këtë lloj nxjerrjeje;

c) Përgatitjen e çdolloj materiali të tillë, të nxjerrë në këtë mënyrë për shitje, me përjashtim të veprimtarive të çfarëdolloj procesi të prodhimit të këtyre materialeve, duke përjashtuar industritë minerare-nxjerrëse nëpërmjet shpimit të përkufizuar në nenin 2 të rregullore “Për kërkesat minimale për mbrojtjen e sigurisë dhe shëndetit të



punëmarrësve në industritë minerare nxjerrëse nëpërmjet shpimit”.

3. “Zonë e rrezikut”, zona në të cilën ka një risk domethënës për sigurinë dhe shëndetin e personave që punojnë aty, për shkak të natyrës së punës që zhvillohet.

4. “Person kompetent”, personi i cili, duke pasur parasysh detyrën që ai kryen, duke marrë në konsideratë përmasat dhe/ose risqet e subjektit në të cilin ai punon, ka formimin, përvojën dhe njohuritë e mjaftueshme, të përshtatshme me natyrën e punës që do të kryhet.

5. “Instalim sipërfaqësor ndihmës”, çdo instalim sipërfaqësor ku ndodhen vendet individuale të punës që janë thelbësore për operimin e një industrie nxjerrëse sipërfaqësore apo nëntokësore.

6. “Kërkimi”, veprimtaria e kërkimit për minerale ose depozita minerale.

7. “Leje e punës”, procedura e dokumentuar, e cila përgatitet dhe nxirret nga personi përgjegjës për vendin e punës, përpara se të fillojë puna, e cila autorizon punëmarrës të veçantë për të kryer punë të veçanta të identifikuar në Dokumentin për Sigurinë dhe Shëndetin në Punë, brenda një periudhe kohore të përcaktuar. Dokumenti për Sigurinë dhe Shëndetin në Punë specifikon kushtet që duhet të përmbushen dhe masat parandaluese që duhen marrë përpara, gjatë dhe pas kryerjes së punës. Ai gjithashtu kërkon që personi përgjegjës të nënshkruajë një deklaratë që puna është përfunduar ose, nëse nuk është e përfunduar, që ajo duhet të vazhdojë përtej afatit të përcaktuar.

8. “Vend pune”, çdo vend në të cilin bëhet një punë apo veprimtari i lidhur me të dhe përfshin të gjithë zonën e synuar për të vendosur vendet individuale të punës, në lidhje me veprimtaritë e drejtpërdrejta e ndihmëse dhe instalimet e çdo industrie minerare-nxjerrëse, sipërfaqësore dhe nëntokësore, përfshirë pirgjet e mbingarkesës dhe grumbujt e tjerë, si dhe çdo akomodim, nëse është ofruar, me kusht që të jenë të aksesueshëm në kontekstin e punës së tyre.

SEKSIONI II

DETYRIMET E PUNËDHËNËSVE

Neni 3

Detyrimet e përgjithshme

1. Për të ruajtur sigurinë dhe shëndetin e

punëmarrësve, punëdhënësi merr masat e nevojshme për të siguruar që:

a) vendet e punës të jenë projektuar, ndërtuar, pajisur, vënë në punë, vënë në funksionim dhe mirëmbajtur në mënyrë të tillë që punëmarrësit të mund të kryejnë punën që u është caktuar pa rrezikuar sigurinë dhe shëndetin e tyre ose atë të punëmarrësve të tjerë në punë;

b) vënia në funksionim e vendeve të punës, kur punëmarrësit janë të pranishëm, të kryhet nën mbikëqyrjen e një personi përgjegjës;

c) puna që përfshin një risk të veçantë të kryhet vetëm nga stafi kompetent dhe në përputhje me udhëzimet e dhëna;

ç) të gjitha udhëzimet e sigurisë të jenë të kuptueshme për të gjithë punëmarrësit;

d) të jenë siguruar mjedise, mjete, pajisje të përshtatshme të ndihmës së parë;

dh) në intervale të rregullta kohore të bëhen ushtrime praktike sigurie.

2. Punëdhënësi përgatit dhe mban të përditësuar një dokument të shkruar, të njohur si Dokumenti i Sigurisë dhe Shëndetit në Punë, i cili përcakton me hollësi të paktën:

a) mënyrën se si punëdhënësi identifikon, vlerëson dhe kontrollon risqet në vendin e punës për të ruajtur sigurinë e shëndetin e punëmarrësve, kur ata punojnë, si dhe sigurinë e shëndetin e personave të tjerë që mund të jenë të pranishëm në vendin e punës, përfshirë klientët, vizitorët dhe publikun;

b) se risqet ndaj të cilave ekspozohen punonjësit në vendin e punës janë përcaktuar dhe vlerësuar;

c) masat e përshtatshme që janë marrë për të arritur këtë, si dhe burimet që janë siguruar për të ruajtur dhe përmirësuar sigurinë e shëndetin.

3. Përveç kërkesave të mësipërme, Dokumenti i Sigurisë dhe Shëndetit në Punë përmban në mënyrë specifike:

a) Në lidhje me nxjerrjen sipërfaqësore dhe nëntokësore të mineraleve:

i) detajet për procedurën për nxjerrjen dhe plotësimin e lejes së punës në përputhje me përcaktimin e bërë në seksionin 1.8, të shtojcës, pjesa A;

ii) detajet për shpeshësinë e regjistrimit dhe dokumentimit të vlerave të përqendrimeve të gazit, të matura nga detektorë automatikë, kur kjo kërkohet sipas përcaktimit të bërë në seksionin 4.1.3, të shtojcës, pjesa A;



iii) planin për parandalimin e shpërthimeve që përcakton me detaje pajisjet dhe masat e nevojshme për sigurinë e shëndetit e punëmarrësve, në përputhje me përcaktimin e bërë në seksionin 4.2.3, të shtojcës, pjesa A;

iv) detaje për masat që do të merren për të parandaluar nisjen dhe përhapjen e zjarreve, në përputhje me përcaktimin e bërë në seksionin 4.4.1, të shtojcës, pjesa A;

v) masat që janë marrë për sigurinë dhe shëndetin e punëmarrësve në situatat si normale ashtu edhe kritike, në përputhje me përcaktimin e bërë në seksionin 1, të pjesës B, dhe në seksionin 1, të pjesës C, të shtojcës së kësaj rregulloreje.

b) Në lidhje me nxjerrjen nëntokësore të mineraleve:

i) detaje të monitorimit të vazhdueshëm të përqendrimeve të ndezshme të gazit në rrugët e kthimit nga njësitë e prodhimit, në përputhje me përcaktimin e bërë në seksionin 8.7, të shtojcës, pjesa C;

ii) të dhëna për vendndodhjen e barrierave të shpërthimit në minierat që përmbajnë pluhur të ndezshëm, sipas përcaktimeve në seksionin 9.4, të shtojcës, pjesa C;

iii) detaje të masave për të identifikuar dhe mbrojtur punëmarrësit dhe për të kontrolluar risqet kur i afrohen punimeve që paraqesin rrezik nga shpërthimet e gazit, shpërthimet e shkëmbinjve dhe vërshimet e llurbave e të ujit.

4. Në rastet kur punëmarrësit nga subjekte të ndryshme janë të pranishëm në të njëjtin vend pune:

a) secili punëdhënës është përgjegjës për të gjitha çështjet nën kontrollin e tij, si dhe duhet të bashkëpunojë me punëdhënësin e ngarkuar për vendin e punës për të koordinuar dhe zbatuar masat e procedurat në lidhje me sigurinë dhe shëndetin e punëmarrësve;

b) punëdhënësi i ngarkuar me vendin e punës është përgjegjës për koordinimin dhe zbatimin e të gjitha masave në lidhje me sigurinë e shëndetin e punëmarrësve dhe dokumenton çdo masë e procedurë për të vënë në jetë koordinimin në dokumentin e tij të Sigurisë dhe Shëndetit në Punë;

c) koordinimi nuk cenon përgjegjësinë e punëdhënësve individualë siç parashikohet në vijim në këtë rregullore dhe ligjin nr. 10237, datë 18.2.2010, “Për sigurinë dhe shëndetin në punë”, dhe ligjin nr. 8741, datë 15.2.2001, “Për sigurinë në punë në veprimtarinë minerare”.

5. Punëdhënësi njofton:

a) çdo aksident në punë, sëmundje profesionale dhe çdo ngjarje të rrezikshme në punë sipas përcaktimeve të legjislacionit në fuqi për sigurinë dhe shëndetin në punë, të RISHM-ja, Inspektorati Shtetëror i Punës, Instituti i Sigurimeve Shoqërore, si dhe Inspektorati Shtetëror që mbulon fushën e shëndetësisë;

b) menjëherë autoritetet kompetente, sipas përcaktimit në ligjin nr. 10237, datë 18.2.2010, “Për sigurinë dhe shëndetin në punë”, ligjin nr. 8741, datë 15.2.2001, “Për sigurinë në punë në veprimtarinë minerare”, dhe rregulloret përkatëse në fuqi, për çdo aksident dhe sëmundje profesionale të rëndë në punë dhe/ose me vdekje, si dhe për çdo situatë të rëndë të rrezikshme.

Nëse është e nevojshme, punëdhënësi përditëson Dokumentin e Sigurisë dhe Shëndetit në Punë duke regjistruar aty çdo masë të marrë për të shmangur çdo përsëritje.

Neni 4

Mbrojtja nga zjarri, shpërthimet dhe atmosferat që rrezikojnë shëndetin

Punëdhënësi merr masa dhe veprime parandaluese të përshtatshme me natyrën e operacionit:

a) për të parandaluar, zbuluar dhe luftuar fillimin dhe përhapjen e zjarreve dhe shpërthimeve;

b) për të parandaluar krijimin e atmosferave shpërthyes dhe/ose që rrezikojnë shëndetin.

Neni 5

Mjetet e largimit dhe shpëtimit

Punëdhënësi siguron dhe mirëmban mjete të përshtatshme të largimit dhe shpëtimit, për të siguruar që punëmarrësit të kenë mundësi të mjaftueshme për t'u larguar nga vendet e punës menjëherë dhe në mënyrë të sigurt në rast rreziku.

Neni 6

Sistemet e komunikimit, paralajmërimit dhe alarmit

Punëdhënësi merr masat e nevojshme për të siguruar praninë e sistemit të paralajmërimit dhe sistemeve të tjera të komunikimit, të nevojshme për të lejuar që dhënia e ndihmës, largimi dhe operacionet e shpëtimit të fillojnë menjëherë, nëse lind nevoja.



Neni 7

Informimi i vazhdueshëm i punëmarrësve

1. Pa cenuar nenin 12, të ligjit nr. 10237, datë 18.2.2010, “Për sigurinë dhe shëndetin në punë”, dhe nenin 11, të ligjit nr. 8741, datë 15.2.2001, “Për sigurinë në punë në veprimtarinë minerare”, punëdhënësi informon punëmarrësit dhe përfaqësuesit e tyre mbi të gjitha masat e marra tashmë dhe për ato që do të merren në lidhje me sigurinë e shëndetin në punë dhe, në veçanti, për ato masa që lidhen me zbatimin e neneve 3 deri në 6 të kësaj rregulloreje.

2. Punëdhënësi siguron që çdo informacion i përmendur në pikën 1, të këtij neni, të jetë i kuptueshëm për punëmarrësit dhe/ose përfaqësuesit e tyre.

Neni 8

Mbikëqyrja shëndetësore

1. Në përputhje me legjislacionin përkatës në fuqi për mbikëqyrjen shëndetësore në punë, punëdhënësi u siguron punëmarrësve mbikëqyrje shëndetësore, të përshtatshme me risqet ndaj sigurisë dhe shëndetit në vendin e punës, të tilla si:

a) risqet fizike, përfshirë zhurmën, dridhjen dhe rrezatimin;

b) risqet nga substanca të rrezikshme, si: kimike, biologjike;

c) risqet psiko-sociale etj.

2. Punëdhënësi merr masa në mënyrë që çdo punëmarrës, të cilit i janë ngarkuar detyra të lidhura me aktivitetet e përmendura në shkronjat “d” dhe “dh”, të nenit 2, të ketë të drejtë për mbikëqyrje shëndetësore:

a) përpara se atij t’i ngarkohen detyra të tilla;

b) më pas në mënyrë periodike dhe sipas nevojës.

3. Punëdhënësi siguron që mbikëqyrja shëndetësore periodike të përfshijë kontrollin periodik në lidhje me:

a) çrregullime të aparatit respirator;

b) çrregullime të aparatit kardio-vaskular;

c) çrregullime muskulo-skeletore;

ç) çrregullime të aparatit urinar;

d) çrregullime të sistemit nervor;

dh) çrregullime të aparatit të dëgjimit;

e) çrregullime të aparatit të shikimit.

Neni 9

Konsultimi dhe pjesëmarrja e punëmarrësve

Punëdhënësi siguron që konsultimi dhe pjesëmarrja e punëmarrësve, si dhe e përfaqësuesve të tyre të zhvillohen në përputhje me nenin 9, të ligjit nr. 10237, datë 18.2.2010, “Për sigurinë dhe shëndetin në punë”, për çështjet që mbulohen nga kjo rregullore.

Neni 10

Kërkesat minimale për sigurinë dhe shëndetin në punë

1. Vendet e punës, që përdoren për herë të parë pas datës në të cilën hyn në fuqi kjo rregullore, plotësojnë kërkesat minimale të sigurisë e të shëndetit, të përcaktuara në shtojcë.

2. Vendet e punës në përdorim përpara datës në të cilën hyn në fuqi kjo rregullore plotësojnë kërkesat minimale të sigurisë e të shëndetit, të përcaktuara në shtojcë sa më shpejt të jetë e mundur dhe jo më vonë se 2 vjet pas kësaj date.

3. Në rastet kur vendet e punës pësojnë ndryshime, zgjerime dhe/ose shndërrime pas datës në të cilën hyn në fuqi kjo rregullore, punëdhënësi merr masa e nevojshme për të siguruar që këto ndryshime, zgjerime dhe/ose shndërrime të jenë në përputhje me kërkesat përkatëse minimale të përcaktuara në shtojcë.

**SEKSIONI III
DISPOZITA TË TJERA**

Neni 11

Sanksionet

Në rast të shkeljes së dispozitave të përcaktuara në këtë rregullore, kur kjo nuk përbën vepër penale, zbatohen sanksionet e përcaktuara në nenin 43, të ligjit nr. 10237, datë 18.2.2010, “Për sigurinë dhe shëndetin në punë”.

Neni 12

Kjo rregullore nuk zbatohet për nxjerrjen e mineraleve përmes larjes së rërave të detit, liqenit ose shtratit të lumit.



SHTOJCË

KËRKESA MINIMALE TË SIGURISË E TË SHËNDETIT, TË PËRMENDURA NË NENIN 10 TË KËSAJ RREGULLOREJE

PJESA A

KËRKESA TË PËRBASHKËTA MINIMALE TË ZBATUESHME PËR INDUSTRIË MINERARE- NXJERRËSE, SIPËRFAQËSORE DHE NËNTOKËSORE, DHE INSTALIMET NDIHMËSE SIPËRFAQËSORE

1. Organizimi dhe mbikëqyrja

1.1. Organizimi i vendit të punës

1.1.1 Punëdhënësi siguron që, për të shmangur risqet e sigurisë dhe shëndetit të punëmarrësve, vendet e punës:

a) të organizohen në mënyrë të tillë që të sigurohet mbrojtja e duhur ndaj risqeve;

b) të mbahen të pastra;

c) të jenë pastruar apo kontrolluar nga çdo substancë ose depozitim i rrezikshëm në to.

1.1.2 Punëdhënësi siguron që vendet individuale të punës të projektohen dhe të ndërtohen në bazë të parimeve ergonomike, duke marrë parasysh nevojën e punëmarrësve për të kryer operacionet në mënyrë të sigurt dhe pa rriske në vendet e tyre individuale të punës.

1.1.3 Punëdhënësi siguron që kur vendet e punës janë të zëna nga punëmarrës të vetmuar, të ofrohet mbikëqyrje ose mjete të komunikimit të mjaftueshme.

1.2 Personi përgjegjës

1.2.1 Punëdhënësi cakton një person kompetent që të jetë përgjegjës për çdo vend pune, në çdo kohë kur janë të pranishëm punëmarrësit.

1.2.2 Përcaktimet sipas pikës 1.2.1 të pjesës A, të kësaj shtojce, nuk e pengojnë punëdhënësin që të caktojë veten e tij si personi përgjegjës nëse ai është kompetent për të marrë përsipër detyrimet që përfshijn ky pozicion.

1.3 Mbikëqyrja

1.3.1. Punëdhënësi cakton një person kompetent, që vepron në emër të punëdhënësit për të ofruar mbikëqyrjen e nevojshme gjatë kryerjes të të gjitha operacioneve për garantimin e sigurisë e të shëndetit të punëmarrësve.

1.3.2 Përcaktimet sipas pikës 1.3.1, të pjesës A, të kësaj pjese nuk e ndalojnë punëdhënësin që të caktojë veten e tij si mbikëqyrës, nëse ai është kompetent për të marrë përsipër detyrat

mbikëqyrëse të përfshira.

1.3.3 Në rastet kur kjo kërkohet nga Dokumenti për Sigurinë dhe Shëndetin në Punë, mbikëqyrësi duhet të vizitojë vendet individuale të punës ku punohet të paktën një herë gjatë çdo turni.

1.4 Punëmarrësit kompetentë

Punëdhënësi siguron që kur në një vend pune janë të pranishëm punëmarrës, aty duhet të ketë një numër të mjaftueshëm prej tyre me aftësitë, përvojën dhe formimin e nevojshëm për të kryer detyrat që u janë caktuar.

1.5. Informimi, formimi dhe udhëzimet

Punëdhënësi:

a) u ofron punëmarrësve informacion, udhëzime, formim dhe riformim për të garantuar sigurinë dhe shëndetin e tyre;

b) siguron që punëmarrësit të marrin udhëzime të kuptueshme, në mënyrë që të mos rrezikohet siguria dhe shëndeti i tyre apo i punëmarrësve të tjerë.

1.6. Udhëzimet me shkrim

Punëdhënësi siguron që:

a) për çdo vend pune të hartohen udhëzime me shkrim që specifikojnë rregullat që duhet të respektohen për të garantuar sigurinë e shëndetin e punëmarrësve dhe përdorimin e sigurt të pajisjeve;

b) udhëzimet me shkrim të përfshijnë informacion për përdorimin e pajisjeve të emergjencës dhe veprimet që duhet të ndërmerren në rast të një emergjence në vendin e punës ose në afërsi të tij;

c) udhëzimet të jepen në formë, mënyrë dhe gjuhë të kuptueshme e të përshtatshme për punëmarrësit.

1.7 Metoda të sigurt të punës

Punëdhënësi siguron që në çdo vend pune ose lidhur me çdo veprimtari të kryer të zbatohen metoda të sigurt të punës.

1.8 Lejet e punës

1.8.1 Kur kjo kërkohet nga Dokumenti i Sigurisë dhe Shëndetit në Punë, punëdhënësi siguron parashikimin e sistemit të lejeve të punës për kryerjen e veprimtarive si të rrezikshme ashtu edhe të drejtpërdrejta, në rastet kur ato mund të ndërveprojnë me veprimtari të tjera për të shkaktuar rreziqe serioze.

1.8.2 Përveç kësaj, punëdhënësi siguron që këto leje pune të lëshohen nga një person përgjegjës përpara fillimit të punës, duke specifikuar kushtet që duhet të plotësohen dhe masat parandaluese që



duhen të merren paraprakisht, gjatë dhe pas punës.

1.9 Rishikimi i rregullt i masave të sigurisë dhe shëndetit

Punëdhënësi siguron që masat e marra për mbrojtjen e sigurisë e të shëndetit të punëmarrësve, përfshirë sistemin e menaxhimit të sigurisë dhe shëndetit, të rishikohen rregullisht për të siguruar respektimin e kësaj rregulloreje.

2. Pajisjet dhe impiantet mekanike dhe elektrike

2.1 Rregulla të përgjithshme

Punëdhënësi siguron që:

a) përzgjedhja, instalimi, vënia në punë, vënia në funksionim dhe mirëmbajtja e pajisjeve mekanike dhe elektrike të bëhen duke i kushtuar rëndësinë e duhur sigurisë e shëndetit të punëmarrësve, duke marrë në konsideratë dispozita të tjera të kësaj rregulloreje dhe të legjislacionit në fuqi mbi konformitetin e makinerive e të pajisjeve dhe vendimin nr. 563, datë 3.7.2013, të Këshillit të Ministrave, “Për kërkesat minimale të sigurisë dhe shëndetit në punë për përdorimin e pajisjeve të punës në vendin e punës”.

b) pajisjet mekanike dhe elektrike, që ndodhen në një zonë brenda së cilës ekziston apo ka gjasa të ekzistojë risku nga zjarri ose shpërthimi si pasojë e ndezjes së gazit, avullit ose lëngut të paqëndrueshëm, të jenë të përshtatshme për t’u përdorur në këtë zonë dhe, nëse është e nevojshme, të pajisen me mjete të përshtatshme mbrojtëse dhe sisteme të sigurt në rast avarie.

2.2 Rregulla të veçanta

2.2.1 Punëdhënësi siguron që:

a) pajisjet dhe impiantet mekanike të kenë forcë të mjaftueshme, të mos kenë defekte të prodhimit dhe të jenë të përshtatshme për qëllimin për të cilin janë destinuar;

b) pajisjet dhe impiantet elektrike të jenë të një madhësie dhe fuqie të mjaftueshme për qëllimin për të cilin ato janë destinuar.

2.2.2 Pajisjet dhe instalimet mekanike dhe elektrike duhet të jenë instaluar dhe të mbrojtura në mënyrë të tillë që të parandalohet rreziku.

3. Mirëmbajtja

3.1. Mirëmbajtja e përgjithshme

Punëdhënësi siguron që:

a) të hartohet një program i përshtatshëm për të ofruar në mënyrë sistematike kontrollin, mirëmbajtjen dhe, kur është e nevojshme, testimin e pajisjeve e të impianteve mekanike dhe elektrike;

b) të gjitha kontrollet, mirëmbajtjet dhe testimet

e çdo pjese të impiantit të kryhen nga një person kompetent;

c) procesverbalet e kontrolleve e të testimeve të kryhen dhe të mbahen në një mënyrë të përshtatshme.

3.2 Mirëmbajtja e pajisjeve të sigurisë

Punëdhënësi siguron që pajisjet e përshtatshme të sigurisë të mirëmbahen në gjendje të gatshme për përdorim dhe në kushte të mira pune në çdo kohë dhe që mirëmbajtja e tyre të kryhet duke pasur parasysh operacionet në zhvillim e sipër.

4. Mbrojtja nga atmosferat e dëmshme, risqet e shpërthimit dhe zjarreve

4.1 Rregulla të përgjithshme

Punëdhënësi siguron që:

a) të merren masa për të vlerësuar praninë e substancave të dëmshme dhe/ose potencialisht shpërthyes në atmosferë, si dhe për matjen e përqendrimit të substancave të tilla;

b) kur kërkohet nga Dokumenti i Sigurisë dhe Shëndetit në Punë të ketë një numër dhe kombinim të përshtatshëm të llojeve të pajisjeve të monitorimit, që masin përqendrimet e gazrave në mënyrë automatike e të vazhdueshme, në vende të specifikuara, si dhe alarme automatike e pajisje për të ndërprerë automatikisht furnizimin me energji të instalimeve elektrike e të motorëve me djegie të brendshme;

c) në rastet kur janë parashikuar matje automatike të përqendrimit të gazrave, vlerat e matura të regjistronen dhe të mbahen sipas përcaktimit të bërë në Dokumentin e Sigurisë dhe Shëndetit në Punë;

ç) të mos lejohet pirja e duhanit në zonat që janë subjekt i risqeve të veçanta të zjarrit apo shpërthimit;

d) të ndalohet çfarëdolloj veprimtarie e punës që kërkon përdorimin e një flake të hapur ose që mund të krijojë risk për ndezje, përveç rasteve kur janë marrë masa të përshtatshme të sigurisë për të parandaluar ndezjen e zjarreve apo shpërthimet.

4.2 Mbrojtja nga risqet për shpërthim

Punëdhënësi siguron që:

a) të merren të gjitha masat e nevojshme për të parandaluar krijimin dhe grumbullimin e atmosferave shpërthyes;

b) në zonat ku ka risqe për shpërthim, të merren të gjitha masat e nevojshme për të parandaluar ndezjen e atmosferave shpërthyes;

c) kur ka një risk për sigurinë dhe shëndetin e



punëmarrësve, Dokumenti i Sigurisë dhe Shëndetit në Punë të përmbajë një plan për parandalimin e shpërthimit i cili përcakton me hollësi pajisjet dhe masat e nevojshme.

4.3 Mbrojtja nga substancat e dëmshme dhe atmosferat e dëmshme

4.3.1 Punëdhënësi siguron që në rastet kur në atmosferë grumbullohen ose mund të grumbullohen substanca të dëmshme, të merren masat e duhura për të siguruar:

- a) bllokimin e tyre në burim;
- b) nxjerrjen ose heqjen e tyre në burim; ose
- c) hollimin e grumbullimeve të substancave të tilla,

në një mënyrë të tillë që përhapja e një substance të tillë të dëmshme të mos i vërë punëmarrësit në risk për sigurinë dhe shëndetin e tyre.

4.3.2 Pa cenuar vendimin nr. 563, datë 3.7.2013, të Këshillit të Ministrave, “Për kërkesat minimale të sigurisë dhe shëndetit në punë për përdorimin e pajisjeve mbrojtëse individuale në vendin e punës”, punëdhënësi siguron pajisje të përshtatshme dhe të mjaftueshme të frymëmarrjes dhe rikthimit në jetë në zonat ku punëmarrësit mund të ekspozohen ndaj atmosferave të cilat janë të dëmshme për shëndetin. Punëdhënësi është përgjegjës për ruajtjen dhe mirëmbajtjen e tyre në mënyrë të përshtatshme.

4.3.3 Punëdhënësi siguron që në zona të tilla, një numër i mjaftueshëm punëmarrësish të formuar për të përdorur këto pajisje të jenë të pranishëm. Kur sulfuri i hidrogenit apo gazra të tjera toksike janë ose mund të jetë të pranishëm në atmosferë, duhet të vihet në dispozicion të autoriteteve kompetente një plan i mbrojtjes që përcakton pajisjet mbrojtëse në dispozicion dhe masat e marra parandaluese.

Punëdhënësi siguron që pajisjet të ruhen dhe të mirëmbahen në mënyrë të përshtatshme.

4.4 Mbrojtja nga rreziqet e zjarrit

Punëdhënësi siguron që:

a) në çdo rast kur vendet e punës janë projektuar, ndërtuar, pajisur, vënë në punë, vënë në funksionim apo mirëmbajtur, të merren masa të mjaftueshme për të parandaluar rënien e zjarreve dhe përhapjen nga burimet e identifikuara në Dokumentin e Sigurisë dhe Shëndetit në Punë;

b) të merren masa për fikje të shpejtë dhe të efektshme të zjarrit;

c) vendet e punës të pajisen me mjete të përshtatshme zjarrfikëse dhe, sipas nevojës, me detektorë të zjarrit dhe sisteme alarmi të vendosura në mënyrë të përshtatshme;

ç) pajisjet joautomatike kundër zjarrit të jenë lehtësisht të arritshme dhe të thjeshta për t’u përdorur dhe, kur është e nevojshme, të mbrohen nga dëmtimi;

d) në vendin e punës të ketë një plan të mbrojtjes nga zjarri që përcakton hollësisht masat paraprake që do të merren, në përputhje me nenet 3, 4, 5 dhe 6, të kësaj rregulloreje, për t’u mbrojtur, zbuluar dhe luftuar shpërthimin e përhapjen e zjarreve;

dh) pajisjet zjarrfikëse të tregohen me shenja në përputhje me vendimin nr. 1012, datë 10.12.2010, të Këshillit të Ministrave, “Për miratimin e rregullores për sinjalistikën në kantier dhe në vendin e punës”. Shenja të tilla vendosen në vende të përshtatshme dhe janë të tilla që i rezistojnë kohës.

5. Lëndët shpërthyesë dhe pajisjet iniciuese

Punëdhënësi siguron që operacionet, që kanë të bëjnë me ruajtjen, transportin, përdorimin dhe asgjësimin e lëndëve shpërthyesë dhe pajisjeve iniciuese, të organizohen dhe të kryhen nga persona të autorizuar në mënyrë të rregullt dhe kompetentë, pa paraqitur risk për punëmarrësit.

6. Rrugët e qarkullimit

Punëdhënësi siguron që:

a) vendet e punës të arrihen pa rrezik dhe largimi prej tyre të mund të kryhet me shpejtësi e në mënyrë të sigurt gjatë një emergjence;

b) rrugët e qarkullimit, përfshirë shkallët, shkallët vertikale të fiksuara, si dhe platformat e rampat ngarkuese, të llogariten, të kenë përmasa dhe të vendosen në mënyrë të tillë që të sigurojnë akses të lehtë, të sigurt e të përshtatshëm për këmbësorët ose mjetet, në mënyrë të tillë që të mos dëmtohen punëmarrësit e punësuar në afërsi të këtyre rrugëve të kalimit;

c) rrugët e përdorura për qarkullimin e këmbësorëve dhe/ose qarkullimin e mallrave të dimensionohen në përputhje me numrin e përdoruesve të mundshëm dhe llojin e subjektit;

ç) në raste kur mjetet e transportit përdoren në rrugët e qarkullimit, për këmbësorët të sigurohet një hapësirë e mjaftueshme sigurie;

d) një hapësirë e mjaftueshme të lejohet ndërmjet rrugëve të qarkullimit të mjeteve dhe



dyerve, portave, kalimeve për këmbësorët, korridoreve dhe shkallëve;

dh) rrugët e qarkullimit dhe të hyrjes të identifikohen qartazi për mbrojtjen e punëmarrësve;

e) kur automjetet apo makinat hyjnë në vendet e punës, hartohen rregullat e trafikut, sipas nevojës.

7. Vendet e punës në mjedis të hapur

7.1 Punëdhënësi siguron që:

a) vendet individuale të punës, rrugët e qarkullimit dhe zona apo instalime të tjera në mjedis të hapur, të cilat përdoren apo janë të zëna nga punëmarrësit gjatë veprimtarisë së tyre, të organizohen në mënyrë të tillë që këmbësorët dhe mjetet të mund të qarkullojnë në mënyrë të sigurt;

b) vendet e punës në mjedise të hapura të ndriçohen në mënyrë të përshtatshme me ndriçim artificial, nëse ndriçimi natyral nuk është i mjaftueshëm.

7.2 Punëdhënësi siguron që kur punëmarrësit punojnë në vende pune individuale në mjedise të hapura, këto vende individuale të punës, sa më shumë të jetë e mundur, të organizohen në mënyrë të tillë që punëmarrësit:

a) të jenë të mbrojtur ndaj kushteve të këqija të motit dhe, nëse është e nevojshme, ndaj objekteve që bien;

b) të mos jenë të ekspozuar ndaj niveleve të dëmshme të zhurmës dhe as ndaj ndikimeve të jashtme të dëmshme, të tilla si gazrat, avujt ose pluhurat;

c) të jenë në gjendje të largohen nga vendi i tyre individual i punës në rast të një rreziku apo të mund të ndihmohen me shpejtësi;

ç) të mos rrëshqasin apo të mos bien.

8. Zonat e rrezikut

Punëdhënësi siguron që:

a) nëse vendet e punës, për shkak të natyrës së punës, përmbajnë zona rreziku në të cilat ka risqe, përshtirë risqet e rënies së punëmarrësve ose të objekteve, vendet të pajisen, me sa është e mundur me mjete që parandalojnë hyrjen e personave të paautorizuar në këto zona;

b) në rastet kur punëmarrësit ose persona të tjerë autorizohen për të hyrë në zonat e rrezikut, të merren masa të përshtatshme për t'i mbrojtur ata nga rreziku;

c) zonat e rrezikut të tregohen në mënyrë të qartë.

9. Rrugët dhe daljet e emergjencës

Punëdhënësi siguron që:

a) në rast të një rreziku, punëmarrësit të kenë mundësi të evakuohen nga të gjitha vendet individuale të punës shpejt dhe në mënyrë të sigurt;

b) rrugët dhe daljet e emergjencës të mbahen të lira dhe të çojnë nëpërmjet mjeteve sa më të drejtpërdrejta jashtë apo në një zonë të sigurt, një pikë të sigurt grumbullimi ose evakuimi;

c) numri, vendndodhja dhe dimensionet e rrugëve e të daljeve të emergjencës të varen nga përdorimi, pajisjet dhe dimensionet e vendeve të punës dhe numri maksimal i personave që mund të jenë të pranishëm;

ç) dyert e emergjencës të hapen nga jashtë ose, nëse kjo është e pamundur, të jenë dyer rrëshqitëse;

d) dyert e emergjencës të mos kyçen apo të mos mbërthehen në mënyrë të tillë që të mos hapen lehtësisht dhe menjëherë nga çdo person që mund të ketë nevojë t'i përdorë ato në një situatë emergjence;

dh) dyert dhe daljet e emergjencës, si dhe rrugët e qarkullimit e dyert që të çojnë tek ato të mos kenë pengesa, në mënyrë që të mund të përdoren pa vështirësi në çdo kohë;

e) rrugët dhe daljet e emergjencës, që kanë nevojë për ndriçim, të pajisen me ndriçim emergjencash me intensitet të mjaftueshëm në rast të një avarie të ndriçimit;

ë) rrugët dhe daljet e veçanta të emergjencës të tregohen me shenja në përputhje me vendimin nr. 1012, datë 10.12.2010, të Këshillit të Ministrave, "Për miratimin e rregullores për sinjalistikën në kantier dhe në vendin e punës".

10. Evakuimi dhe largimi

Punëdhënësi siguron:

a) formimin e punëmarrësve për veprimet që duhet të kryhen në raste emergjencash;

b) që pajisjet e shpëtimit të jenë në vende të dukshme dhe të arritshme, të vendosen në mënyrë të përshtatshme dhe të mbahen në gjendje të gatshme për përdorim, si dhe të tregohen me shenja në përputhje me vendimin nr. 1012, datë 10.12.2010, të Këshillit të Ministrave, "Për miratimin e rregullores për sinjalistikën në kantier dhe në vendin e punës".

11. Ushtrimet praktike të sigurisë

Punëdhënësi siguron që ushtrimet praktike të sigurisë të kryhen në intervale të rregullta në të gjitha vendet e punës në të cilat punëmarrësit janë zakonisht të pranishëm.



Qëllimi kryesor i këtyre ushtrimeve praktike të sigurisë është për të formuar dhe kontrolluar aftësitë e punëmarrësve, të cilëve u janë caktuar detyra të veçanta në rast të një emergjence, që përfshin funksionimin, përdorimin, mirëmbajtjen dhe manipulimin e pajisjeve të emergjencës, duke marrë parasysh kriteret e përcaktuara në Dokumentin e Sigurisë dhe Shëndetit në Punë.

12. Dhomat dhe pajisjet e ndihmës së parë Punëdhënësi siguron që:

a) pajisjet e ndihmës së parë të jenë të pranishme në të gjitha vendet ku kjo kërkohet nga kushtet e punës dhe të jenë të përshtatshme për përdorim;

b) pajisjet e ndihmës së parë të jenë të shënjuara në mënyrë të përshtatshme dhe lehtësisht të arritshme;

c) një ose më shumë dhoma të ndihmës së parë të jenë siguruar kur madhësia e ndërtesave, lloji i veprimtarisë që zhvillohet dhe frekuenca e aksidenteve e diktojnë një gjë të tillë;

ç) udhëzimi për administrimin e ndihmës së parë në rast të një aksidenti të jetë afishuar në mënyrë të qartë në dhomat e ndihmës së parë;

d) dhomat e ndihmës së parë të jenë të pajisura me instalime dhe pajisje bazë të ndihmës së parë dhe të jenë lehtësisht të arritshme për barelat;

dh) dhomat e ndihmës së parë të jenë shënjuar në përputhje me vendimin nr. 1012, datë 10.12.2010, të Këshillit të Ministrave, “Për miratimin e rregullores për sinjalistikën në kantier dhe në vendin e punës”;

e) përveç pajisjeve në dhomat e ndihmës së parë, në të gjitha vendet ku diktohet nga kushtet e punës, të jenë të disponueshme pajisje të ndihmës së parë që janë të shënjuara në mënyrë të përshtatshme;

ë) një numër i mjaftueshëm i punëmarrësve të formohen lidhur me përdorimin e pajisjeve të ndihmës së parë.

13. Ndryshimi natyror dhe artificial¹

Punëdhënësi siguron që:

a) çdo vend pune të pajiset kudo me ndriçim të mjaftueshëm për të garantuar sigurinë dhe shëndetin e personave që ndodhen aty;

b) vendet e punës, sa më shumë të jetë e mundur, të marrin ndriçim natyror të mjaftueshëm dhe të jenë pajisur, duke marrë në konsideratë kushtet klimaterike, me ndriçim artificial të mjaftueshëm për mbrojtjen e sigurisë e të shëndetit të punëmarrësve;

c) instalimet e ndriçimit në dhomat ku ndodhen vendet e punës dhe në rrugët e kalimit të vendosen në mënyrë të tillë që lloji i ndriçimit të mos paraqesë një risk aksidenti për punëmarrësit;

ç) vendet e punës në të cilat punëmarrësit janë veçanërisht të ekspozuar ndaj risqeve, sidomos në rastin e avarive të ndriçimit artificial, të pajisen me ndriçim emergjence me intensitet të përshtatshëm.

14. Mjediset dhe pajisjet sanitare

14.1 Dhomat e zhveshjes dhe dollapët personale

Punëdhënësi siguron që:

a) punëmarrësit të kenë dhoma të përshtatshme për t’u ndërruar, nëse ata duhet të veshin rroba të veçanta pune dhe kur për arsye të shëndetit ose të etikës atyre nuk mund t’u kërkohet të ndërrohen në një vend tjetër. Dhomat e zhveshjes duhet të jenë lehtësisht të arritshme, të kenë kapacitete të mjaftueshme dhe të jenë të pajisura me ndenjëse;

b) dhomat e zhveshjes të jenë mjaftueshëm të mëdha dhe të kenë ambiente për t’i krijuar mundësi çdo punëmarrësi për të kyçur veshjet e tij gjatë orarit të punës;

c) nëse rrethanat e kërkojnë, dollapët personale për veshjet e punës të jenë të ndara nga ato për veshjet e zakonshme, si dhe merr masa për të tharë veshjet e lagura;

ç) dhomat e zhveshjes për burrat dhe gratë të jenë të ndara;

d) nëse dhomat e zhveshjes nuk kërkohen sipas pikës 14.1/a, çdo punëmarrësi t’i sigurohet një vend për të vendosur veshjet e tij.

14.2 Dushet dhe lavamanët

14.2.1 Nëse kjo kërkohet nga natyra e punës dhe për arsye shëndetësore, punëdhënësi siguron dushë të mjaftueshme dhe të përshtatshme për punëmarrësit, të cilat janë:

a) në dhoma dushi të ndara apo me përdorim të veçantë për burrat dhe gratë;

b) brenda dhomave të dusheve me standarde higjienike dhe të pajisura me ujë të rrjedhshëm, të ngrohtë e të ftohtë, si dhe me madhësi të mjaftueshme për t’i dhënë mundësi çdo punëmarrësi që të lahet pa pengesa.

14.2.2 Punëdhënësi siguron që, kur dhomat në të cilat ndodhen dushet apo lavamanët, të cilat janë siguruar në përputhje me seksionin 14.2.1, janë të ndara nga dhomat e zhveshjes, të ketë komunikim të lehtë ndërmjet të dyjave.

14.2.3 Në rastet kur dushet nuk kërkohen sipas



seksionit 14.2, punëdhënësi siguron lavamanë të mjaftueshëm e të përshtatshëm, me ujë të rrjedhshëm, të ngrohtë e të ftohtë, në afërsi të vendit individual të punës dhe dhomave të zhveshjes.

Lavamanët të jenë të ndarë apo të përdoren veçmas nga burrat dhe gratë, kur kjo kërkohej për arsye të etikës.

14.3 WC-të dhe lavamanët

Punëdhënësi siguron që në afërsi të vendeve individuale të punës, dhomave të çlodhjes, dhomave të zhveshjes dhe dhomave ku ndodhen dushet dhe lavamanët të ketë hapësira me një numër të përshtatshëm të WC-ve dhe lavamanëve, veçmas apo me përdorim të veçantë për burrat dhe gratë. Në rastin e industrive minerare-nxjerrëse nëntokësore, instalimet sanitare të përmendura në këtë seksion mund të vendosen në sipërfaqe.

15. Pirgjet dhe grumbujt e tjerë

Punëdhënësi siguron që pirgjet, grumbujt me mbeturina, dampat e sterileve dhe grumbujt të tjerë të projektohen, të ndërtohen, të vihen në funksionim dhe të mirëmbahen në një mënyrë që siguron qëndrueshmërinë e tyre, si dhe sigurinë e shëndetit e punëmarrësve.

16. Instalimet sipërfaqësore ndihmëse (dispozita të veçanta shtesë)

16.1 Qëndrueshmëria dhe fortësia

Punëdhënësi siguron që vendet e punës:

a) të projektohen, të ndërtohen, të montohen, të vihen në funksionim, të mbikëqyren dhe të mirëmbahen në mënyrë që t'i rezistojnë forcave mjedisore të pritshme;

b) të kenë një strukturë dhe fortësi të përshtatshme me natyrën e përdorimit të tyre.

16.2 Dyshemetë, muret, tavanet e çatitë e dhomave

Punëdhënësi siguron që:

a) dyshemetë e vendeve të punës të mos kenë gunga, të çara ose pjerrësi të rrezikshme dhe të jenë të fiksuara, të qëndrueshme dhe jo të rrëshqitshme;

b) vendet e punës, ku ndodhen vendet individuale të punës, të izoloohen në mënyrë të përshtatshme kundër të nxehtit, duke pasur parasysh llojin e ndërmarrjes së përfshirë dhe veprimtarinë fizike të punëmarrësve;

c) sipërfaqet e dyshemeve, mureve dhe tavaneve në dhoma të jenë të tilla që të mund të pastrohen dhe të riparohen në një standard të përshtatshëm të higjienës;

ç) muret transparente apo që lejojnë depërtimin e dritës, në veçanti ndarjet tërësisht prej qelqi, në dhoma ose në afërsi të vendeve të punës dhe rrugëve të lëvizjes, të tregohen qartazi dhe të përbëhen nga materiale të sigurta. Në vende dhe rrugë kalimi të tilla të ketë mburoja për të mos lejuar kontaktin e punëmarrësve me këto mure ose lëndimin e tyre në rast se këto mure thyhen;

d) hipja në çatitë që përbëhen nga materiale me fortësi të pamjaftueshme të mos lejohet përveç rasteve kur janë siguruar pajisje që garantojnë që puna të kryhet në një mënyrë të sigurt.

16.3 Dimensionet e dhomave dhe hapësira ajrore në dhoma-liria e lëvizjes në vendin individual të punës

Punëdhënësi siguron që:

a) dhomat e punës të kenë sipërfaqe, lartësi dhe hapësirë ajrore të mjaftueshme për të lejuar punëmarrësit që të kryejnë punën e tyre pa rriske për sigurinë, shëndetin apo mirëqenien e tyre;

b) dimensionet e hapësirave të lira në vendin individual të punës t'u lejojnë punëmarrësve liri lëvizjeje të mjaftueshme dhe t'u japin mundësi atyre të kryejnë punën e tyre në mënyrë të sigurt.

16.4 Dritaret dhe çatitë prej xhami

Punëdhënësi siguron që:

a) dritaret, çatitë prej xhami dhe pajisjet e ajrimit, të cilat janë të destinuara për t'u hapur, përshtatur dhe siguruar, të projektohen dhe të montohen në mënyrë të tillë që këto operacione të mund të kryhen në mënyrë të sigurt dhe të vendosen në mënyrë të tillë që nuk përbën rrezik për punëmarrësit gjatë përdorimit;

b) të jetë e mundur që dritaret dhe çatitë prej xhami të pastrohen pa ndonjë risk.

16.5 Dyert dhe portat

Dyert dhe portat

Punëdhënësi siguron që:

a) pozicioni, numri dhe dimensionet e dyerve e të portave, si dhe materialet e përdorura për ndërtimin e tyre të përcaktohen sipas natyrës dhe përdorimit të dhomave ose zonave;

b) dyert transparente të shënohen në mënyrë të përshtatshme në nivelin e syrit;

c) dyert dhe portat rrrotulluese ose lëkundëse të jenë transparente ose të kenë pjesë të tejdukshme;

ç) në rastet kur sipërfaqet transparente apo të tejdukshme në dyer dhe porta nuk përbëhen nga materiale të sigurta dhe ekziston risku që punëmarrësit të mund të dëmtohen nëse ato



thyhen, sipërfaqet e dyerve apo portave të mbrohen kundër thyerjeve;

d) dyert e rrëshqitshme të pajisen me një pajisje të sigurisë për të parandaluar daljen e tyre nga shinat dhe rënien e tyre në mënyrë të papritur;

dh) dyert dhe portat që hapen nga jashtë të pajisen me një mekanizëm për t'i siguruar ato kundër lëvizjeve mbrapa në mënyrë të papritur;

e) dyert përgjatë rrugëve të largimit të shënjohen në mënyrë të përshtatshme dhe të jetë e mundur që ato të hapen nga brenda në çdo kohë pa ndihmë të veçantë kur vendet e punës janë në përdorim;

ë) për këmbësorët të sigurohen dyer të veçanta në vendet ngjitur me çdo portë që është synuar kryesisht për qarkullimin e mjeteve, përveç rasteve kur kalimi i këmbësoreve përmes tyre është i sigurt dhe këto dyer janë shënuar qartazi dhe lihen pa pengesa gjatë gjithë kohës;

f) dyert dhe portat mekanike të funksionojnë pa risk për aksident për punëmarrësit dhe të jenë pajisur me mjete stakimi të emergjencës lehtësisht të identifikueshme dhe të arritshme, përveç rasteve kur ato hapen automatikisht dhe në rast të një avarie të furnizimit me energji të jetë gjithashtu e mundur që ato të hapen manualisht;

g) në rastet kur zinxhirë apo pajisje të ngjashme përdoren për të parandaluar aksesin në çfarëdolloj vendi, ato të jenë qartazi të dukshme dhe të identifikueshme në mënyrë të përshtatshme, me anë të shenjave që tregojnë çdo ndalim ose paralajmërim.

16.6 Ajrimi i vendeve të mbyllura të punës

Ajrimi i vendeve të mbyllura të punës

Punëdhënësi siguron që:

a) të ketë ajër të freskët të mjaftueshëm në vendet e mbyllura të punës, duke pasur parasysh metodat e përdorura të punës dhe kërkesat fizike për punëmarrësit;

b) në rastet kur përdoret një sistem ajrimi mekanik, ai të mbahet në gjendje funksionale dhe çdo avari të tregohet nga një sistem kontrolli, kur kjo është e nevojshme për shëndetin e punëmarrësve;

c) kur përdoren instalime të kondicionimit të ajrit apo të ajrimit mekanik, ato duhet të funksionojnë në mënyrë të tillë që punëmarrësit të mos jenë të ekspozuar ndaj rrymave të ajrit që shkaktojnë parehati dhe që çdo grumbullim ose papastërti, që ka gjasa të krijojë risk të menjëhershëm për shëndetin e punëmarrësve duke ndotur atmosferën, të hiqet pa vonesë.

16.7 Temperatura e dhomës

Punëdhënësi siguron që:

a) temperatura në dhomat ku ndodhen vendet individuale të punës të jetë e përshtatshme për organizmin e njeriut gjatë kohës së punës, duke pasur parasysh metodat e punës që përdoren dhe ngarkesat fizike që i janë vendosur punëmarrësve;

b) temperatura në mjediset e pushimit, dhomat e personelit që kryen shërbim të vazhdueshëm, ambientet sanitare, mensat dhe dhomat e ndihmës së parë t'i përshtatet qëllimit të posaçëm që kanë këto hapësira;

c) dritaret, çatitë prej xhami dhe ndarëset prej qelqi të lejojnë shmangien e pasojave të tepruara nga ndriçimi i diellit mbi vendet e punës, duke pasur parasysh llojin dhe vendin e punës.

16.8 Dhomat e çlodhjes

Përveç rasteve kur punëmarrësit punojnë në zyra apo dhoma pune të ngjashme që ofrojnë çlodhje ekuivalente gjatë pushimeve, punëdhënësi siguron që:

a) punëmarrësit të kenë një dhomë çlodhjeje që është lehtësisht e arritshme në rastet kur siguria ose shëndeti i punëmarrësve, në veçanti, lloji i veprimtarisë së zhvilluar ose prania e më shumë se një numri të caktuar punëmarrësish e kërkojnë një gjë të tillë;

b) dhomat e çlodhjes të jenë të pajisura me numër të mjaftueshëm tavolinash dhe karrigesh me mbështetëse dhe të jenë mjaftueshëm të mëdha për numrin e punëmarrësve;

c) nëse oraret e punës ndërpriten rregullisht e shpesh dhe nuk ka dhoma çlodhjeje, të ofrohen dhoma të tjera në të cilat punëmarrësit mund të qëndrojnë gjatë këtyre ndërprerjeve, sa herë që kjo kërkohet për sigurinë dhe shëndetin e punëmarrësve;

ç) të ndalohet pirja e duhanit në dhomat e çlodhjes ose në dhomat e tjera të siguruar për punëmarrësit në të cilat ata mund të qëndrojnë gjatë ndërprerjeve të punës.

17. Gratë shtatzëna dhe nënat me fëmijë me gj

Punëdhënësi siguron që gratë shtatzëna dhe nënat me fëmijë me gjë të kenë mundësinë të shtrihen për të pushuar në kushte të përshtatshme.

18. Punëmarrësit me aftësi të kufizuara

Punëdhënësi siguron që vendet e punës të organizohen duke marrë parasysh punëmarrësit me aftësi të kufizuara, veçanërisht në lidhje me dyert, rrugët e kalimit, shkallët, dushet, lavamanët, WC-të



dhe vendet individuale të punës të përdorura ose të zëna drejtpërdrejt nga persona me aftësi të kufizuara.

PJESA B

KËRKESA TË VEÇANTA MINIMALE TË ZBATUESHME PËR INDUSTRI TË MINERARE NXJERRËSE SIPËRFAQËSORE

1. Rregulla të përgjithshme

1.1 Pa cenuar nenin 3 (2) të kësaj rregulloreje, punëdhënësi përgjegjës për vendin e punës të mbuluar nga kjo pjesë B, duhet të sigurojë që Dokumenti për Sigurinë dhe Shëndetin në Punë të tregojë se janë marrë të gjitha masat për mbrojtjen e sigurisë dhe shëndetit të punëmarrësve në situatë normale dhe kritike.

1.2 Punëdhënësi siguron që Dokumenti i Sigurisë dhe Shëndetit në Punë të përditësohet rregullisht dhe të jetë i disponueshëm për inspektim në vendin e punës dhe puna të kryhet në përputhje me dokumentin për sigurinë dhe shëndetin.

2. Funksionimi

Punëdhënësi siguron që:

a) puna të planifikohet duke marrë në konsideratë elementet e Dokumentit të Sigurisë dhe Shëndetit në Punë, që kanë të bëjnë me risqet për rënie apo rrëshqitje të tokës, dhe në veçanti lartësinë e pjerrësinë e zhveshjes së shtresës së sipërme e të anëve të nxjerrjes që duhet të jenë të përshtatshme me natyrën dhe qëndrueshmërinë e tokës e metodat e punës;

b) shpatet dhe sheshet e shkalleve të jenë mjaftueshëm të qëndrueshme për makineritë e përdorura, të ndërtohen dhe të mirëmbahen në një mënyrë që makineritë të lëvizin në mënyrë të sigurt;

c) përpara fillimit ose rifillimit të punës të kryhet kontrolli për struktura shkëmbore të paqëndrueshme për sipërfaqet dhe shpatet e shkalleve mbi zonën ku punohet, duke përfshirë zonën ku punohet dhe rrugët e lëvizjes;

ç) shpatet e shkalleve dhe stoqet e grumbullimit të bëhen në mënyrë të tillë që të mos krijohet paqëndrueshmëri.

PJESA C

KËRKESA TË VEÇANTA MINIMALE TË ZBATUESHME PËR INDUSTRI TË MINERARE NXJERRËSE NËNTOKËSORE

1. Në përgjithësi

1.1 Pa cenuar nenin 3 (2) të kësaj rregulloreje,

punëdhënësi, i cili është përgjegjës për vendin e punës të mbuluar nga kjo pjesë C, duhet të sigurojë që Dokumenti për Sigurinë dhe Shëndetin në Punë të tregojë se janë marrë të gjitha masat përkatëse për mbrojtjen e sigurisë e të shëndetit të punëmarrësve në situatë normale dhe kritike.

1.2 Punëdhënësi siguron që Dokumenti i Sigurisë dhe Shëndetit në Punë të përditësohet rregullisht dhe të jetë i disponueshëm për inspektim në vendin e punës dhe që aktivitetet e punës të kryhen në përputhje me Dokumentin e Sigurisë dhe Shëndetit në Punë.

2. Planimetritë e punimeve nëntokësore

Punëdhënësi siguron që:

a) të përgatiten planimetritë e punimeve nëntokësore të cilat janë vizatuar në një shkallë e cila siguron një pasqyrim të qartë të rrugëve dhe të zonave ku kryhen punime minerare dhe të çdo elementi të njohur që mund të influencojnë sigurinë e operacioneve që kryhen;

b) planimetritë të jenë gjithmonë të aksesueshme dhe të mbahen për sa kohë është e nevojshme për qëllime sigurie;

c) planimetritë e punimeve nëntokësore të përditësohen rregullisht dhe të mbahen të disponueshme në vendin e punës.

3. Daljet

Punëdhënësi siguron që:

a) të gjitha punimet nëntokësore të kenë akses në sipërfaqe me të paktën dy rrugëdalje të ndara të cilat janë ndërtuar mirë dhe janë lehtësisht të arritshme nga punëmarrësit që ndodhen nën tokë.

b) kur lëvizja e punëmarrësve kërkon përpjekje të konsiderueshme fizike, punëdhënësi të vërë në dispozicion mjete dhe pajisje të transportit mekanik.

4. Punimet minerare nëntokësore

Punëdhënësi siguron që:

a) punimet minerare nëntokësore të ndërtohen, të vihen në funksionim, të pajisen dhe mirëmbahen në një mënyrë që punëmarrësit të mund të punojnë dhe lëvizin në to me një risk minimal;

b) rrugët duhet të pajisen me sinjalistikë për të ndihmuar punëmarrësit që të lëvizin lehtësisht në punimet minerare nëntokësore.

5. Transporti

Punëdhënësi siguron që:

a) mjetet dhe pajisjet e transportit të jenë instaluar, të jenë vënë në funksionim dhe të mirëmbahen në një mënyrë të tillë që garanton



sigurinë dhe shëndetin e drejtuesve, përdoruesve dhe personave të tjerë në afërsi;

b) mjetet dhe pajisjet e transportit mekanik apo vagonët për njerëz të jenë instaluar siç duhet dhe të përdoren në përputhje me udhëzimet me shkrim.

6. Mbajtja e punimeve minerare dhe qëndrueshmëria e shkëmbinjve

Punëdhënësi siguron që:

a) mbajtja e punimeve minerare të bëhet sa më shpejt të jetë e mundur pas gërmimit, përveç rasteve kur qëndrueshmëria e shkëmbinjve e bën të panevojshme për sigurinë e punëmarrësve, me përjashtim të rasteve kur qëndrueshmëria e tokës e bën të panevojshme për sigurinë dhe shëndetin e punëmarrësve. Mbështetja duhet të instalohet në përputhje me planet dhe udhëzimet me shkrim;

b) armaturat të jenë të vendosura në përputhje me projektet dhe udhëzimet me shkrim;

c) punimet minerare ku kryhet aktivitet minierar nga punëmarrësit të inspektohen rregullisht për qëndrueshmërinë e shkëmbinjve dhe mbajtja e tyre të ruhet në përputhje me këtë.

7. Ajrimi

Punëdhënësi siguron që:

a) të gjitha punimet minerare nëntokësore të cilat lejohet aksesimi dhe që janë në aktivitet të ajrosen në një mënyrë të vazhdueshme dhe me një shkallë të përshtatshme të sigurisë për të ruajtur:

i) një atmosferë të shëndetshme;

ii) një atmosferë, në të cilën risqet e shpërthimit dhe pluhurat e thithshme mbahen nën kontroll;

iii) një atmosferë në të cilën kushtet e punës janë të përshtatshme gjatë kohës që puna është në zhvillim, duke pasur parasysh metodat e punës që përdoren dhe kërkesat fizike të vendosura ndaj punëmarrësve.

b) kur kërkesat e shkronjës “a” nuk mund të përmbushen nëpërmjet ajrimit natyral, ajrimi kryesor të sigurohet nëpërmjet një ose më shumë ventilatorësh mekanikë për të siguruar ajrim të qëndrueshëm dhe të vazhdueshëm;

c) depresioni i ventilatorëve kryesorë monitorohet në mënyrë të vazhdueshme dhe një alarm automatik të tregojë ndalimet e paplanifikuara;

ç) parametrat e ajrimit të maten dhe të regjistrohen në mënyrë periodike;

d) një projekt i ajrimit, që përmban detajet përkatëse të sistemit të ajrimit, të përgatitet, të përditësohet dhe të mbahet periodikisht në vendin e punës.

8. Minierat me gaz

Punëdhënësi siguron që:

a) minierat dhe punimet nëntokësore të konsiderohen me gaz, në qoftë se gazi i minierës ose gaze të tjerë potencialisht të ndezshëm kanë dalë ose ka gjasa të dalin në një sasi të tillë që risku i krijimit të një atmosfere shpërthyes nuk mund të përjashtohet dhe që kërkesat në vijim të këtij seksioni të përmbushen;

b) ajrimi kryesor të sigurohet nga një ose më shumë ventilatorë mekanikë;

c) punimet të vazhdojnë duke marrë parasysh emetimin e gazit të minierës apo gazeve të tjerë të djegshëm dhe të jenë marrë hapat e nevojshëm për të eliminuar sa më shumë të jetë e mundur risqet që rrjedhin nga gazrat e ndezshme;

ç) ajrimi ndihmës i vendeve të punës të kufizohet në:

i) punimet minerare për hapjen e minierës dhe riaktivizimin e punimeve të veçanta,

ii) vende me një lidhje të drejtpërdrejtë me rrymën kryesore të ajrimit.

d) punimet e prodhimit të ajrosen nga sisteme ndihmëse vetëm nëse janë marrë masat e duhura shtesë për të garantuar sigurinë dhe shëndetin e punëmarrësve;

dh) për çdo matje të ajrimit të kërkuar nga pika 7 (ç) përcaktohet përqendrimi i gazit të ndezshëm;

e) kur marrja e këtij hapi është përcaktuar si e nevojshme nga Dokumenti i Sigurisë dhe Shëndetit në Punë, nivelet e gazit të ndezshëm të monitorohen gjithashtu vazhdimisht në rrymat e ajrit që kthehen nga njësia e prodhimit, duke përfshirë vendet e punës ku përdoren mekanizma dhe punimet minerare qorre;

ë) për minierat me gaz përdoren vetëm eksplozivë dhe pajisje iniciuese të posaçme;

f) dispozitat e pikës 4.1 (b) të pjesës A zëvendësohen, si më poshtë:

- ndalohet pirja e duhanit, mbajtja e duhanit për pirjen e tij dhe çdo objekt i cili mund të përdoret për të prodhuar flakë;

g) dispozitat e pikës 4.1 (d) të pjesës A zëvendësohen, si më poshtë:

- prerja me flakë, saldimi dhe operacione të tjera të ngjashme lejohen vetëm në rrethana të jashtëzakonshme dhe në bazë të masave specifike që garantojnë sigurinë dhe shëndetin e punëmarrësve.



9. Minierat e qymyrit që përmbajnë pluhura të ndezshme

Punëdhënësi siguron që:

a) minierat e qymyrit të konsiderohen si të prirura ndaj pluhurave të ndezshme, përveç rasteve kur Dokumenti i Sigurisë dhe Shëndetit në Punë tregon se asnjë nga shtresat që po punohen nuk përmban pluhur që mund të shkaktojë përhapjen e ndonjë shpërthimi;

b) kur minierat janë të prekshme nga pluhurat e ndezshme, dispozitat e pikave 8 (dh) dhe 8 (e) të kësaj pjese C, zbatohen pavarësisht nga prania e gazrave të ndezshme;

c) të merren masa për të ulur grumbullimet e pluhurit të ndezshëm për të hequr holluar dhe neutralizuar ato;

ç) përhapja e pluhurit të ndezshëm dhe/ose shpërthimeve të gazit të minierës, të cilat janë shkaktare të nxitjes së shpërthimeve të mëtejshme të pluhurit të ndezshëm, të kufizohen duke instaluar një sistem barrierash të shpërthimit dhe duke treguar vendndodhjet e këtyre barrierave të shpërthimit në Dokumentin e Sigurisë dhe Shëndetit në Punë, i cili përditësohet periodikisht dhe mbahet i disponueshëm në vendin e punës.

10. Shpërthime të gazit, shembjet e shkëmbinjve dhe vërshimet e ujit

Punëdhënësi siguron që:

a) në zonat e prirura për shpërthime të gazit me ose pa flakjen e mineraleve apo shkëmbinjve, shembjet e shkëmbinjve dhe vërshimet e ujit, në përputhje me Dokumentin e Sigurisë dhe Shëndetit në Punë, të hartohet dhe të zbatohet plani i veprimit, në mënyrë që të sigurohet, sa më shumë të jetë e mundur një sistem i sigurt i punës dhe mbrojtja e punëmarrësve.

b) plani i veprimit i përmendur në shkronjën “a” përfshin masa për identifikimin e zonave të riskut për të mbrojtur punëmarrësit në punimet minerare të cilave u afrohen, punojnë dhe lëvizin nëpërmjet tyre dhe për të kontrolluar risqet.

11. Zjarret, djegiet dhe nxehjet

Punëdhënësi siguron:

a) marrjen e masave për parandalimin dhe, kur është e përshtatshme, zbulimin e hershëm të djegieve spontane;

b) kufizimin e sasisë së materialeve të ndezshme të çuara në punimet nëntokësore në sasi të që janë ekzaktësisht të nevojshme;

c) që kur është i nevojshëm përdorimi i lëngjeve hidraulike për transmetimin e energjisë, për sa është e mundur, lëngje të tilla që ndizen me vështirësi, plotësojnë specifikimet e kushtet e testimit ndaj zjarrit, si dhe kriteret higjienike;

ç) kur lëngjet hidraulike që përdoren nuk i plotësojnë specifikimet, kushtet dhe kriteret e përmendura në shkronjën “c” të merren masa parandaluese shtesë për të shmangur rrezikun e shtuar të zjarrit dhe përhapjen e tij.

12. Masat parandaluese për largimin e punëmarrësve

Punëdhënësi siguron që:

a) kur është e nevojshme punëmarrësve t'u sigurohen mjete mbrojtëse të vetëshpëtimit të mbrojtjes së frymëmarrjes, të cilat ata duhet t'i mbajnë gjithmonë brenda rrezes së aksesit të tyre në mënyrë që ata të mund të tërhiqen në mënyrë të sigurt;

b) punëmarrësit të formohen lidhur me përdorimin e mjeteve mbrojtëse të vetëshpëtimit të frymëmarrjes;

c) mjetet mbrojtëse të vetëshpëtimit të frymëmarrjes të qëndrojnë në kantier dhe të kontrollohen e të mirëmbahen rregullisht për të siguruar që ato janë në kushte të mira.

13. Ndriçimi

Dispozitat e seksionit 13 të pjesës A zëvendësohen, si më poshtë:

Punëdhënësi siguron që:

a) punëmarrësit të pajisen me një llambë personale të përshtatshme;

b) vendet individuale të punës sa më shumë të jetë e mundur të pajisen me ndriçim artificial të mjaftueshëm për mbrojtjen e sigurisë dhe shëndetit të punëmarrësve;

c) instalimet e ndriçimit të vendosen në mënyrë të tillë që të mos ketë risk aksidenti për punëmarrësit si pasojë e llojit të ndriçimit të vendosur.

14. Evidentimi i punëmarrësve dhe personave të tjerë nën tokë

Punëdhënësi siguron që në çdo kohë të jetë e mundur të dihet me saktësi kush është nën tokë nga punëmarrësit dhe persona të tjerë.

15. Organizimi i shpëtimit

Punëdhënësi siguron një organizim të përshtatshëm të shpëtimit për të mundësuar ndërmarrjen e veprimeve të përshtatshme me shpejtësi dhe efektivitet në rast të një incidenti



madhor, i cili, në mënyrë që të mund të veprojë në çdo vend ku punohet në punimet minerare nëntokësore të nxjerrjes ose hapjes, ka në dispozicion një numër të mjaftueshëm punëmarrësish të trajnuar të shpëtimit si dhe pajisje adekuate për këtë qëllim.

VENDIM

Nr. 973, datë 2.12.2015

PËR MIRATIMIN E DOKUMENTIT TË POLITIKAVE PËR SIGURINË KIBERNETIKE 2015–2017

Në mbështetje të nenit 100 të Kushtetutës, me propozimin e ministrit të Shtetit për Inovacionin dhe Administratën Publike, Këshilli i Ministrave

VENDOSI:

1. Miratimin e dokumentit të politikave për sigurinë kibernetike 2015-2017, sipas tekstit bashkëngjitur këtij vendimi.

2. Ngarkohen ministri i Shtetit për Inovacionin dhe Administratën Publike dhe ministrinë e institucionet qendrore, të përmendura në tekstin e këtij dokumenti, për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

**KRYEMINISTRI
Edi Rama**

DOKUMENTI I POLITIKAVE PËR SIGURINË KIBERNETIKE 2015–2017 REPUBLIKA E SHQIPËRISË TIRANË, 2015

Lista e shkurtimeve

AKCE	Autoriteti Kombëtar i Certifikimit Elektronik
AKEP	Autoriteti i Komunikimeve Elektronike e Postare
AKSHI	Agjencia Kombëtare e Shoqërisë së Informacionit
ALCIRT	Agjencia Kombëtare për Sigurinë Kompjuterike
ASPA	Shkolla Shqiptare për Administratën Publike
BE	Bashkimi Evropian
DSIK	Drejtoria e Sigurimit të Informacionit të Klasifikuar
ENISA	Agjencia e Bashkimit European për Sigurinë e Rrjeteve dhe Informacionit (ang. European Union Agency for Network and Information Security)
FIRST	Forumi i Ekipeve të Përgjigjes ndaj Incidenteve dhe Sigurisë(ang. Forum for Incident Response and Security Teams)
ISP	Ofruesit e Shërbimit të Internetit (ang. Internet Service Provider)
IZHA	Instituti i Zhvillimit të Arsimit
KDIMDP	Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale
ITU	Unioni Ndërkombëtar i Telekomunikacioneve
MD	Ministria e Drejtësisë
MSHIAP	Ministër Shteti për Inovacionin dhe Administratën Publike
MM	Ministria e Mbrojtjes
MPB	Ministria e Punëve të Brendshme
NATO	Organizata e Traktatit të Atlantikut Verior (ang. North Atlantic Treaty Organization)
PSH	Policia e Shtetit
SHISH	Shërbimi Informativ Shtetëror
TAIEX	Asistenca Teknike për Shkëmbimin e Informacionit (ang. Technical Assistance Information Exchange)
TF-CIRT	Task Forca e Ekipeve të Përgjigjes ndaj Incidenteve Kompjuterike (ang. Task Force Computer Incidence Response Team)



TIK	Teknologjia e Informacionit dhe Komunikimit
IMPACT	Partneriteti Shumëpalësh Ndërkombëtar Kundër Kërcënimeve Kibernetike (ang. International Multilateral Partnership Against Cyber Threats)
VKM	Vendim i Këshillit të Ministrave
CIRT	Ekipi i përgjigjes ndaj incidenteve kompjuterike (ang. Computer Incident Response Team)
CERT	Ekipi i përgjigjes ndaj emergjencave kompjuterike (ang. Computer Emergency Response Team)
CSIRT	Ekipi i përgjigjes ndaj incidenteve të sigurisë kompjuterike (ang. Computer Security Incident Response Team)
GOVNET	Rrjeti Qeveritar (ang. Government Network)
CIIP	Mbrojtja e Infrastrukturave Kritike të Informacionit (ang. Critical Information Infrastructure Protection)

PËRKUFIZIME

“Sistem kompjuterik” do të thotë çdolloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave.

“Të dhëna kompjuterike” do të thotë çfarëdolloj përfaqësimi të fakteve, informacioni apo konceptesh në një formë të përshtatshme për procesim në një sistem kompjuterik, që përfshijnë një program të përshtatshëm për punën e një sistemi kompjuterik për të kryer një funksion.

Shënim. Përkufizimet e mësipërme janë marrë nga ligji nr. 8888, datë 25.4.2002, “Për ratifikimin e “Konventës për krimin në fushën e kibernetikës”

“Rrjet kompjuterik” konsiderohet një rrjet telekomunikimi që i lejon kompjuterët të shkëmbejnë të dhëna.

“Të dhëna personale”² është çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social.

“Shërbim i komunikimeve elektronike”³ është shërbimi, normalisht përkundrejt një pagese, i cili përftohet, tërësisht ose pjesërisht, nga përcjellja e sinjaleve përmes rrjeteve të komunikimeve elektronike, që përfshin shërbimet e telekomunikacioneve dhe shërbimet e transmetimit në rrjetet e përdorur për transmetime radiotelevizive dhe në rrjetet e televizionit kabllor, por duke përjashtuar shërbimet, të cilat ofrojnë përmbajtje nëpërmjet rrjeteve dhe shërbimeve të komunikimeve elektronike, ose që ushtrojnë kontroll redaksional ndaj përmbajtjes së ofruar për transmetimin, duke përdorur rrjetet dhe shërbimet e komunikimeve elektronike. Ai nuk përfshin shërbimet e shoqërisë së informacionit, të cilat nuk përbëhen, tërësisht ose pjesërisht, nga përcjellja e sinjaleve në rrjetet e komunikimeve elektronike.

“Hapësirë kibernetike” konsiderohet hapësira virtuale globale e të gjithë sistemeve të informacionit dhe të komunikimit të ndërlidhur në nivel të dhënash.

“Kërcënim/sulm kibernetik” konsiderohet çdo përpjekje e drejtuar/qëllimshme për të marrë akses, manipuluar, ndërhyrë ose dëmtuar integritetin, konfidencialitetin, sigurinë dhe/ose disponibilitetin e të dhënave, të një aplikimi ose të të dhënave të sistemit kompjuterik, pa pasur autoritet ligjor për ta bërë këtë.

“Krim kibernetik” konsiderohet ndërhyrje e paautorizuar drejt dhe/ose përmes përdorimit të TIK, penalizimi për të cilin rregullohet në Kodin Penal të Republikës së Shqipërisë.⁴

² Ligji nr. 9887, datë 10.3.2008, i ndryshuar, “Për mbrojtjen e të dhënave personale”.

³ Ligji nr. 9918, datë 19.5.2008 “Për komunikimet elektronike në Republikën e Shqipërisë”.

⁴ Ligji nr. 9859, datë 21.1.2008, “Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995, “Kodi Penal i Republikës së Shqipërisë”, të ndryshuar.

Ligji nr. 10023, datë 27.11.2008, “Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995, “Kodi Penal i Republikës së Shqipërisë”, të ndryshuar.

Ligji nr. 10054, datë 29.12.2008, “Për disa shtesa dhe ndryshime në ligjin nr. 7905, datë 21.3.1995, “Kodi i Procedurës Penale i Republikës së Shqipërisë”, të ndryshuar.

Ligji nr. 144/2013, “Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995, “Kodi Penal i Republikës së Shqipërisë”, të ndryshuar.



“Infrastruktura kritike të informacionit” konsiderohen sistemet dhe rrjetet e informacionit dhe komunikimit, cenimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë, dhe/ose mirëqenien ekonomike të qytetarëve, dhe/ose funksionimin efektiv të ekonomisë të Republikës së Shqipërisë.

“Luftë kibernetike” konsiderohet çdo akt luftime në dhe/ose përreth hapësirës kibernetike që lidhet kryesisht me teknologjinë e informacionit.

“Spiunazh kibernetik” konsiderohet sulmi kibernetik që ka si objekt të tij cenimin e konfidencialitetit të një sistemi TIK (p.sh. spiunimi dixhital).

“Sabotazh kibernetik” konsiderohet sulmi kibernetik që ka si objekt të tij cenimin e integritetit dhe disponueshmërisë së një sistemi TIK.

Shënim. Në këtë dokument vetëm për efekt standardizimi në mënyrën e të shprehurit fjala “kompjuterike” dhe “kibernetike” do të konsiderohen ekuivalente.

HYRJE

Me zhvillimet e shpejta të teknologjisë së informacionit dhe komunikimit, me shtrirjen e përdorimit të saj pothuajse në të gjitha fushat e veprimtarisë së shoqërisë, bëhet evidente kërkesa për shërbime të sigurta dhe të besueshme. Rritja e përdorimit të TIK dhe internetit po ndryshon shoqërinë duke krijuar mënyra të reja të lidhjes, komunikimit, bashkëpunimit dhe të zhvillimit ekonomik nëpërmjet aksesit në hapësirën kibernetike. Kjo ka bërë që shoqëria jonë të varet gjithnjë e më shumë në përdorimin e këtyre teknologjive.

Shqipëria renditet ndër vendet ku zhvillimi i telekomunikacionit, qasja në internet dhe informatizimi i shoqërisë përparon shumë shpejt. Rritja e përdorimit të komunikimit përbën një vlerë të shtuar në zhvillimin ekonomik dhe shoqëror të vendit, por, në të njëjtën kohë, ajo e ekspozon atë ndaj rreziqeve të natyrës kibernetike me aktorë shtetërorë dhe jo shtetërorë. Sulmet kibernetike kanë potencial për të dëmtuar rëndë shkëmbimin e informacionit në institucionet publike, të telekomunikacionit dhe sistemin financiar e bankar, duke shkaktuar edhe ndërprerje të shërbimeve jetike.⁵

Aksesi në hapësirën kibernetike së bashku me elementet pozitive të tij rrit rrezikun potencial nga dëmtimi apo keqpërdorimi i të dhënave dhe sistemeve kompjuterike. Si pasojë e rreziqeve kibernetike në rritje, sigurimi i integritetit të të dhënave dhe konfidencialitetit si dhe një akses i sigurt në hapësirën kibernetike, janë kthyer në një nga sfidat më të mëdha me të cilat përballet shoqëria në ditët e sotme duke e kthyer atë në një çështje të sigurisë kombëtare.

Ky Dokument është në mbështetje të Programit të ri të investimeve në TIK të qeverisë shqiptare:

- Përmirësimi i shërbimeve ndaj publikut;
- Një shoqëri informacioni e sigurt; si dhe

Strategjinë e Sigurisë Kombëtare 2014–2020 (cit. “..për vendosjen dhe respektimin e standardeve më të larta në drejtim të ruajtjes dhe mbrojtjes së informacionit në të gjitha trajtat e ekzistencës së tij, duke përqendruar përpjekje të veçanta për mbrojtjen nga sulmet kibernetike”).

Ky dokument është, gjithashtu, në linjë me Agjendën Dixhitale për Evropën 2020 (cit. Rritja e besimit në TIK nëpërmjet forcimit të politikës së sigurisë për rrjetet dhe informacionin) si dhe në linjë me Strategjinë për Sigurinë Kibernetike të Bashkimit Evropian: Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur (ang. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*).

Qëllimi i këtij Dokumenti Politikash është të rishikojë dhe të koordinojë detyrimet që lindin nga angazhimet e marra për një hapësirë kibernetike të sigurt me qëllim që të sigurohet përmbushja e përgjegjësisë nga të gjithë aktorët në mënyrë të koordinuar. Në këtë mënyrë mund të garantohet zhvillimi i mëtejshëm i shoqërisë së informacionit si një ambient i sigurt, i besueshëm dhe i hapur si dhe promovimin e vlerave dhe mundësive të ofruara nga përdorimi i hapësirës kibernetike.

Dokumenti pas një analize të situatës dhe zhvillimeve aktuale, përcakton vizionin dhe objektivat e zhvillimit për periudhën 2015–2017, si dhe jep drejtimet kryesore të politikave që do të ndiqen për realizimin

⁵ Strategjia e Sigurisë Kombëtare (SSK), 2014–2020.



e këtyre objektivave. Dokumenti mbështetet në modelet dhe praktikat më të mira evropiane, për sa u përket objektivave dhe zgjidhjeve të parashikuara, gjithnjë duke marrë në konsideratë karakteristikat specifike të shoqërisë dhe ekonomisë shqiptare.

Ky Dokument Politikash është i shoqëruar dhe me një plan veprimi, i cili do të jetë objekt rishikimi të paktën një herë në vit. Dokumentet kryesore ku është mbështetur Dokumenti i Politikave për Sigurinë Kibernetike 2015–2017, janë:

- Axhenda Dixhitale e Shqipërisë (2014–2020);
- Strategjia e Sigurisë Kombëtare (SSK);
- Strategjia për Sigurinë Kibernetike e Bashkimit Evropian: Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur (ang. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*)⁶.

Në hartimin e këtij dokumenti kanë marrë pjesë të gjitha palët e interesit nga sektori publik dhe privat, si dhe është ndihmuar nga ekspertët e Bashkimit Evropian përmes misionit të TAIEX-it.

Situata aktuale në Shqipëri

Strategjia Ndërsektoriale për Shoqërinë e Informacionit 2008–2013 (SNSHI) e miratuar me VKM nr. 59, datë 21.1.2009, përveçse përbën dokumentin strategjik që përcaktonte drejtimit kryesore dhe objektivat e zhvillimit në fushën e shoqërisë së informacionit për periudhën 2008–2013 ishte edhe dokumenti i vetëm ku përmendej shkurtimisht siguria kibernetike si një nga fushat që duhej konsideruar me prioritet për shkak të vizionit të Qeverisë shqiptare për të rritur e zhvilluar e-qeverisjen përmes ofrimit të e-shërbimeve.

Siguria kompjuterike përmendej në Iniciativat në Fushën e Shoqërisë së Informacionit në SNSHI, si më poshtë:

- Siguria e fëmijëve *online* dhe nxitja e koordinimi i procesit për kodet e sjelljes;
- Krijimi i Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT)
- Krijimi i infrastrukturës PKI dhe ofrimi i shërbimeve të sigurt

Në mbështetje me ligjin “Për mbrojtjen e të drejtave të fëmijëve”, “Planin e veprimit për fëmijë 2012–2015”, miratuar me vendim të Këshillit të Ministrave nr. 182, datë 13.3.2012, legjislacionin shqiptar në fuqi dhe praktikën më të mirë evropiane në këtë drejtim; “Parimet për rrjete sociale më të sigurt për vendet e BE-së”, të Komisionit Evropian publikuar në shkurt të vitit 2009, si dhe dokumentin “Kudri Evropian për një përdorim më të sigurt të Celularit nga adoleshentët dhe fëmijët”, nënshkruar nga operatorë të ndryshëm në Evropë, në shkurt të vitit 2007; më 7 shkurt 2013, u nënshkrua nga operatorë shqiptarë “Kodi i sjelljes për përdorimin e sigurt dhe të përgjegjshëm të rrjeteve dhe të shërbimeve të komunikimeve elektronike në Shqipëri”.

Gjithashtu, në zbatim të Strategjisë Ndërsektoriale për Shoqërinë e Informacionit 2008–2013 (SNSHI), Agjencia Kombëtare e Shoqërisë së Informacionit ka ofruar:

- Autentifikim dhe identifikim të sigurt – për 25 institucione, 2500 përdorues;
- Internet të sigurt për 65 institucione;
- Instalim automatik dhe qendror të aplikimeve – 2000 PC të Ministrave që janë në domain;
- Menaxhim qendror i mbrojtjes antivirus – 7 institucione, 1000 kompjuterë;
- E-signature përmes Infrastrukturës Qeveritare të Çelësit Publik (PKI) – 2 institucione.

Përdorimi i Teknologjisë së Informacionit dhe Komunikimit është rritur ndjeshëm në vitet e fundit. Sipas të dhënave të publikuara nga AKEP, numri i përdoruesve aktivë të shërbimeve celulare në fund të vitit 2013 ishte afërsisht 3.7 milion përdorues. Penetrimi i telefonisë celulare bazuar në kartat SIM aktive arriti në 130%.

Akresi *broadband Internet* ka pasur rritje të ndjeshme si për lidhjet *broadband* fiks me 14% gjatë vitit 2013, ashtu dhe në *mobile broadband*, respektivisht për lidhjet me kartë modem dhe USB me 88–101% gjatë vitit 2013. Në total numri i pajtimtarëve *broadband* (fiks e mobile) është rritur me 36% gjatë vitit 2013.

Numri total i lidhjeve *broadband* fiks në fund të vitit 2013 arriti në 182.556 dhe përdorues të shërbimeve *broadband* bazuar në celular arriti në fund të vitit 2013 në 1.231.269.

⁶ Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - Join(2013) 1 final - 7/2/2013



Përdoruesit e Internetit në Shqipëri janë rritur me disa herë në vitet e fundit. Sipas të dhënave të publikuara nga Bashkimi Ndërkombëtar i Telekomunikacionit, penetrimi i Internetit në Shqipëri në dhjetë vitet e fundit është rritur nga 0.97% në vitin 2003 në mbi 60% në vitin 2013.⁷

Viti	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Shqipëria	0.97	2.42	6.04	9.61	15.04	23.86	41.20	45.00	49.00	54.66	60.10

Ndërkohë që numri i shkeljeve të sigurisë së rrjeteve dhe sigurisë së informacionit është duke u rritur me shpejtësi. Kjo shkakton humbje financiare dhe krijon rreziqe dhe kërcënime të reja për zhvillimin e Shoqërisë së Informacionit. Në këtë kuadër është e domosdoshme që të ndërmerren hapa për zhvillim të sigurt të Shoqërisë së Informacionit.

Nga të dhënat zyrtare të Policisë së Shtetit mbi krimin kibernetik, të rregulluar sipas Kodit Penal të Republikës së Shqipërisë, rezultojnë se në periudhën janar - dhjetor 2014 janë evidentuar 180 vepra penale, janë zbuluar 76, me 86 autorë, nga të cilët 74 janë në gjendje të lirë, 10 të arrestuar dhe 2 në kërkim. Për periudhën janar – dhjetor 2013, janë evidentuar 108 vepra penale nga të cilat janë zbuluar 63 prej tyre, me 69 autorë, nga të cilët 58 janë në gjendje të lirë, 9 arrestuar dhe 2 në kërkim.

Krahasuar me të njëjtën periudhë të vitit të kaluar, janë evidentuar 66% më shumë vepra penale, me 17 autorë më shumë, 1 autor të arrestuar më shumë.

Të ndara sipas veprave penale ato paraqiten si më poshtë:

- Neni 119/a, “Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik”, evidentuar 1 rast, pa autor;

- Neni 143/b, “Mashtrimi kompjuterik”, evidentuar 49 raste, me 14 autorë në gjendje të lirë, 1 i arrestuar;

- Neni 186/a, “Falsifikim kompjuterik”, evidentuar 28 raste, me 20 autor, nga të cilët 4 arrestuar dhe 16 në gjendje të lirë;

- Neni 192/b, “Hyrja e paautorizuar kompjuterike”, evidentuar 14 raste, me 7 autorë në gjendje të lirë;

- Neni 293/a, “Përgjimi i paligjshëm i të dhënave kompjuterike”, evidentuar 1 rast me 2 autorë, në gjendje të lirë;

- Neni 293/b, “Ndërhyrja në të dhënat kompjuterike”, evidentuar 33 raste me 16 autorë, nga të cilët 2 të arrestuar dhe 14 në gjendje të lirë;

- Neni 293/c, “Ndërhyrja në sistemet kompjuterike”, evidentuar 4 raste, me 3 autorë në gjendje të lirë;

- Neni 121 “Ndërhyrje të padrejta në jetën private”, 4 raste, pa autor;

- Neni 117, paragrafi i tretë, “Pornografia”, evidentuar 38 raste me 14 autorë në gjendje të lirë;

- Neni 121/a “Përndjekja”, evidentuar 4 vepër penale, zbuluar 3, me 2 autorë të proceduar në gjendje të lirë, 1 i arrestuar;

- Neni 137/a “Vjedhja e rrjetit të komunikimeve elektronike”, evidentuar 1 vepër penale, zbuluar 1, me 1 autor në gjendje të lirë;

- Neni 149/a “Shkelja e të drejtave të pronësisë industriale”, evidentuar 1 vepër penale, zbuluar 1, me 1 autor i cili është proceduar në gjendje të lirë.

- Shpifja, e parashikuar nga neni 120 i Kodit Penal, evidentuar 1 rast me 1 autor në gjendje të lirë.

⁷ Burimi: <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>



Këto vepra penale të ndara sipas drejtimeve:

Nr.	Krime kompjuterike	Evidentuar	Zbuluar	Autorë gjithsej	Arrestuar	Gjendje të lirë	Larguar
1	Në fushën e teknologjisë dhe informacionit	53	29	30	2	28	-
2	Nëpërmjet sistemit kompjuterik	127	47	56	8	50	-
3	Gjithsej	180	76	86	10	78	-

Sipas drejtorive të policisë së qarqeve, veprat penale të evidentuara ndahen si më poshtë:

Nr.	Drejtoria e Policisë së Qarkut	VP të evidentuara	VP të zbuluara	Autorë Gjithsej	Arrestuar e ndaluar	Në gjendje të lirë
1	Durrës	7	1	1	-	1
2	Korça	4	2	2	-	2
3	Dibër	1	-	-	-	-
4	Berat	1	-	-	-	-
5	Fier	5	4	4	-	4
6	Elbasan	5	4	4	-	4
7	Shkodër	9	3	3	-	3
8	Kukës	2	2	3	3	-
9	Lezhë	3	3	3	-	3
10	Tiranë	61	27	31	6	25
11	Vlorë	6	4	5	-	5
12	Qendra	77	27	30	1	29
	Shuma krime kompjuterike	181	77	86	10	76

Rëndësi të veçantë merr iniciimi i ndryshimeve ligjore në mënyrë që të ofrohet mbrojtje e përshtatshme për përdoruesit, për të rritur besimin e tyre në teknologjitë e informacionit dhe për të inkurajuar përdorimin e avancuar dhe të sigurt të TIK-ut.

Vlerësohet si tejet e nevojshme marrja e veprimeve dhe masave specifike për të ndërgjegjësuar shoqërinë lidhur me rreziqet potenciale në fushën e sigurisë së rrjeteve dhe sistemeve për eliminimin e këtyre rreziqeve, përfshirë mbrojtjen e fëmijëve nga përmbajtjet e paligjshme në hapësirën kibernetike.

Sulmet në infrastrukturën kritike të informacionit në rang vendi mund të kenë pasoja të rënda në funksionalitetin e tyre duke shkaktuar edhe humbje të mëdha financiare, prandaj lind nevoja që së pari ato të identifikohen e më pas të merren masa të forta sigurie për ta mbajtur në nivel më të lartë sigurinë e këtyre infrastrukturave si më jetike për funksionimin e shoqërisë.⁸

Kuadri ligjor dhe institucional

Zhvillimi i shpejtë i TIK-ut kushtëzohet dhe nga përshtatja e legjislacionit përkatës të nevojshëm. Në përgjithësi Shqipëria është në pajtueshmëri me detyrimet që rrjedhin nga MSA-ja në këtë fushë. Ka disa ligje që rregullojnë ndjekjen penale të krimeve kompjuterike në Republikën e Shqipërisë si: ligji nr. 8888 i datës 25.4.2002, “Për ratifikimin e Konventës për Krimin Kibernetik” është reflektuar në Kodin Penal si dhe ligji nr. 9262 i datës 29.7.2004, “Për ratifikimin e Protokollit shtesë të Konventës për krimin kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike” sërish është reflektuar në Kodin Penal përkatësisht në ligjin nr. 9859, datë 21.1.2008 “Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995”, “Kodi Penal i Republikës së Shqipërisë” dhe ligji nr. 10023, datë 27.11.2008 për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995, “Kodi Penal i Republikës së Shqipërisë; dhe ligji nr. 10054, datë 29.12.2008, “Për disa shtesa dhe ndryshime në ligjin nr. 7905, datë 21.3.1995”.⁹

⁸ Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - Join(2013) 1 final - 7/2/2013

⁹ Për ndryshime të mëtejshme në Kodin Penal, referoju ligjit nr. 144/2013, “Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 “Kodi Penal i Republikës së Shqipërisë”, të ndryshuar.

**Kuadri ligjor i strukturave qeveritare që merren me sigurinë dhe krimin kibernetik në Shqipëri**

Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT), është autoriteti qendror për identifikimin, parashikimin dhe marrjen e masave për mbrojtjen ndaj kërcënimeve/sulmeve kompjuterike, në përputhje me legjislacionin në fuqi.

Drejtoria e Sigurimit të Informacionit të Klasifikuar (DSIK), është autoriteti që kontrollon, garanton sigurinë e sistemeve të klasifikuara të komunikimit dhe informacionit dhe bën akreditimin e tyre nëpërmjet lëshimit të Certifikatës së Sigurisë për këto të fundit.

Autoriteti Kombëtar për Certifikimin Elektronik (AKCE), është autoriteti që ka përgjegjësinë e mbikëqyrjes së zbatimit të ligjit [“Për nënshkrimin elektronik”](#) dhe të akteve nënligjore të nxjerra në zbatim të tij. AKCE-ja bën akreditimin e ofruesve të shërbimit të certifikimit elektronik.

Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI), është përgjegjëse për administrimin e infrastrukturës qeveritare të Çelësit Publik (PKI) dhe siguron pajtueshmërinë me nenin 19 të ligjit nr. 9880, datë 25.2.2008, “Për nënshkrimin elektronik”. Në shërbimet që ofron në Qendrën e të Dhënave Qeveritare, për administratën publike, garanton autentifikim dhe identifikim të sigurt, internet të sigurt dhe DNS të sigurt.

Policia e Shtetit, është organi përgjegjës për parandalimin, zbulimin dhe hetimin e veprave penale, ndër të cilat përfshihen dhe veprat penale në fushën e TIK-ut, që ndiqen nga Sektori i Kundër Krimit Kompjuterik.

Prokuroria e Përgjithshme, përmes sektorit të krimeve kibernetike ushtron ndjekjen penale për vepra penale në fushën e kibernetikës. Kjo strukturë kontrollon aktivitetin e njësive të posaçme për ndjekjen e krimeve kibernetike, që janë ngritur në prokuroritë e rretheve gjyqësore.

Shërbimi Informativ i Shtetit (SHISH), përmes seksionit të Kundër Krimit Kibernetik, ka për detyrë kërkimin, zbulimin dhe analizimin e krimeve kibernetike që cenojnë sigurinë kombëtare.¹⁰

Ministria e Mbrojtjes, ka rol në ruajtjen e sigurisë kibernetike përmes Drejtorisë së Automatizimit dhe Inovacionit, por edhe institucioneve të përmendura më poshtë në varësi të Ministrit të Mbrojtjes (DSH dhe AISM).

Shtabi i Përgjithshëm i Forcave të Armatosura të Republikës së Shqipërisë, Drejtoria e Ndërlidhjes, përgjigjet për zhvillimin e Sistemeve të ndërlidhjes dhe të Informacionit (SNI) në Forcat e Armatosura të Republikës së Shqipërisë duke u mbështetur në standardet kombëtare, të NATO-s dhe ato ndërkombëtare.

Drejtoria e Shifrës (DSH), është Autoriteti Kombëtar për Sigurimin e Komunikimeve dhe Autoritet Kombëtar i Shpërndarjes.

Agjencia e Inteligjencës së Mbrojtjes dhe Sigurisë (AISM), përmes sektorit të Mbrojtjes Kibernetike dhe Infosec ka si detyrë parashikimin, identifikimin dhe analizimin e kërcënimeve kibernetike që cenojnë sistemet TIK të FASH-së.

Banka e Shqipërisë (BSH), ka autoritetin e organit që ka të drejtën ekskluzive të japë miratimin për fillimin e aktivitetit bankar nëpërmjet dhënies së licencës, si dhe të mbikëqyrë aktivitetin e çdo subjekti, i cili ka marrë licencë për ushtrimin e veprimtarisë bankare në Republikën e Shqipërisë. Në fushën e sigurisë së sistemeve të tij TIK, subjekti përcakton objektiva, strategji dhe kërkesa të sigurisë, si dhe miraton procedura për administrimin, për operimin, për ruajtjen e sistemeve, për mbrojtjen e të dhënave si edhe për nxjerrjen jashtë përdorimit të tyre.

Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP), mbikëqyr, kontrollon dhe monitoron veprimtaritë e sipërmarrësve të rrjeteve të komunikimeve elektronike dhe të shërbimeve të komunikimeve të elektronike. AKEP-i, mbikëqyr zbatimin e masave të nevojshme të ndërmarra nga

¹⁰ Ligj nr. 8457, datë 11.2.1999, “Për informacionin e klasifikuar “Sekret shtetëror”.

VKM nr. 922 datë 19.12.2007, “Për sigurimin e informacionit të klasifikuar “Sekret Shtetëror” që prodhohet, ruhet, përpunohet apo transmetohet në sistemet e komunikimit (INFOSEC)”.

VKM nr. 690, datë 5.10.2011 “Për miratimin e rregullores “Për mbrojtjen kriptografike të informacionit të klasifikuar “Sekret Shtetëror””.



sipërmarrësit mbi sigurinë dhe integritetin e shërbimeve dhe rrjeteve të komunikimeve elektronike publike në lidhje me mbrojtjen e të dhënave personale.

Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (KDIMDP), është autoriteti përgjegjës i pavarur, që mbikëqyr dhe monitoron, në përputhje me ligjin, mbrojtjen e të dhënave personale elektronike gjatë ruajtjes, përpunimit dhe transmetimit të tyre, duke respektuar e garantuar të drejtat dhe liritë themelore të njeriut.

Institucione të tjera mbështetëse në arritjen e objektivave të Dokumentit

Shkolla Shqiptare e Administratës Publike (ASPA), është organi që ka si detyrë formimin, trajnimin profesional të nëpunësve të administratës të cilat fokusohen në ngritjen e kapaciteteve menaxhuese të qëndrueshme; rritjen e përgjegjshmërisë së punonjësve të administratës; krijimin e një trupe funksionarësh publikë profesionistë, të paanshëm dhe eficientë në kryerjen e funksioneve të tyre. Ky institucion do të ofrojë ndihmë për organizimin e trajnimeve për profesionistët IT të administratës publike.

Instituti i Zhvillimit të Arsimit (IZHA), është institucioni që ka si detyrë hartimin e kurrikulës së TIK-ut për arsimin parauniversitar (k-12), e cila përmban tematika shumë të rëndësishme, të fushës së sigurisë kibernetike, përmbajtja e të cilave konsiston në përdorimin e sigurt të internetit nga nxënësit dhe mësuesit.

Në bazë të VKM-së nr. 303, datë 31.3.2011, “Për krijimin e njësisë të teknologjisë së informacionit e të komunikimit në ministritë e linjës dhe institucionet e varësisë” çdo institucion ka Drejtori TI, e cila është përgjegjëse për sigurinë në sistemet e TIK-ut dhe në këtë kuadër ka edhe përgjegjësi për sigurinë kibernetike.

Vizioni, parimet dhe objektivat strategjike

KY DOKUMENT PËRCAKTON SI VIZION:

Për një hapësirë kibernetike më të sigurt, më të besueshme dhe më të qëndrueshme për qytetarët, biznesin dhe qeverinë në mbështetje të zhvillimit ekonomik dhe social të Shqipërisë.

Hapësira kibernetike duhet parë si një fushë shumë dimensionale, me shumë shtresa dhe gjerësi territoriale përtej kufijve kombëtarë. Realizimi i një sigurie kibernetike duhet të mbështetet në këto parime bazë:

- Mbrojtja e të drejtave themelore të njeriut, lirinë e shprehjes, të dhënat personale dhe privatësinë: Siguria kibernetike mund të jetë efikase vetëm nëse ajo është e bazuar në të drejtat dhe liritë themelore të njeriut sipas Kartës së të Drejtave Themelore të Bashkimit Evropian dhe vlerave thelbësore të BE-së. Reciprokisht, të drejtat e individëve nuk mund të sigurohen pa rrjete dhe sisteme të sigurta. Çdo shkëmbim informacioni, kur përfshin të dhënat personale, duhet të jetë në përputhje me ligjin e mbrojtjes së të dhënave të BE-së, si dhe ligjin nr. 9887, datë 10.3.2008, i ndryshuar, “Për mbrojtjen e të dhënave personale” dhe të marrë parasysh të drejtat e individëve në këtë fushë.

- Akses për të gjithë: Akses i kufizuar dhe/ose pamundësia për akses në internet, si dhe analfabetizmi dixhital përbëjnë një disavantazh për qytetarët, duke pasur parasysh sesa bota dixhitale përshkon veprimtarinë brenda shoqërisë. Çdo njeri duhet të jetë në gjendje të aksesojë internetin dhe të ketë rrjedhë të pakufizuar informacioni. Integriteti dhe siguria e internetit duhet të jenë të garantuara për të lejuar akses të sigurt për të gjithë.

- Përgjegjësi e përbashkët: Siguria kibernetike nuk mund të konsiderohet si një problem i cili prek apo i takon një institucioni, institucioneve shtetërore, sektorit privat ose qytetarëve. Ajo është problem i cili prek gjithë fushat e jetës dhe shoqërisë. Si i tillë kërkon marrjen e masave të nevojshme të sigurisë nga të gjithë përdoruesit e teknologjisë TIK dhe hapësirës kibernetike.

- Forcimi i bashkëpunimit dhe koordinimit: Bazuar në përgjegjësitë e përbashkëta është e nevojshme rritja e bashkëpunimit dhe e koordinimit mes të gjithë aktorëve. Forcimi i bashkëpunimit ndërinstitucional, bashkëpunimi me sektorin privat dhe publik, bashkëpunimi me botën akademike janë të domosdoshme për të arritur qëllimin.



- Bashkëpunimi ndërkombëtar: Hapësira kibernetike si një hapësirë pa kufij kërkon një bashkëpunim dhe koordinim ndërkombëtar për të garantuar sigurinë kibernetike. Gjithashtu, me anëtarësimin në NATO dhe progresin e bërë drejt anëtarësimit në BE, Shqipëria gjithnjë e më shumë është pjesë aktive e iniciativave dhe programeve të sigurisë kibernetike dhe duhet të përmbushë angazhimet e saj ndaj vendeve aleate.

- Administrimi i rrezikut: Rritja e përdorimit të TIK-ut dhe tendenca për një botë gjithnjë e më të ndërlidhur rrit dhe rreziqet me të cilat përballemi. Shqipëria do të marrë masat e nevojshme për administrimin e rrezikut bazuar në standardet dhe praktikatat më të mira për të garantuar sigurinë kibernetike.

- Respektimi i vlerave: Ky dokument do të shërbejë si orientim për marrjen e të gjithë masave, hartimin e politikave, standardeve, udhëzimeve dhe procedurave për të siguruar një mbrojtje ndaj rreziqeve kibernetike duke respektuar në çdo moment parimet e të drejtave dhe lirive themelore, si dhe parime të tjera demokratike.

Objektivat strategjikë që do të ndiqen për përmbushjen e këtij vizioni dhe respektimin e parimeve të mësipërme janë:

- i) plotësimi i kuadrit ligjor në fushën e sigurisë kibernetike;
- ii) forcimi i kuadrit institucional;
- iii) rritja e ndërgjegjësimit për sigurinë kibernetike
- iv) identifikimi dhe mbrojtja e Infrastrukturave Kritike të Informacionit
- v) krijimi dhe implementimi i kërkesave minimale të sigurisë kibernetike
- vi) forcimi i partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit
- vii) rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike.

Politikat për t'u ndjekur

Plotësimi i kuadrit ligjor në fushën e sigurisë kibernetike

Në përputhje me zhvillimet dhe iniciativat do të ndërmerren hapat e nevojshëm për të analizuar, përshtatur dhe plotësuar legjislacionin në fushën kibernetike. Në mënyrë të vazhdueshme do të bëhet vlerësimi i praktikave më të mira botërore, rekomandimeve dhe iniciativave ndërkombëtare të fushës në mënyrë të veçantë ato të NATO-s dhe BE-së, duke përshtatur masat në fushën e sigurisë kibernetike në përputhje me angazhimet e marra ndaj partnerëve ndërkombëtarë. Nëse do të konsiderohet e nevojshme do të bëhet përshtatja dhe miratimi i tyre duke garantuar kështu forcimin e sigurisë kibernetike dhe luftën kundër krimit kibernetik. Në analizën e kryer në funksion të këtij Dokumenti rezulton se kuadri ekzistues ligjor dhe institucional ka disa paqartësi të cilat duhen adresuar, gjatë plotësimit të legjislacionit, si më poshtë:

a) Modernizimin e legjislacionit në fuqi dhe rishikimin periodik të tij për të adresuar sigurinë kibernetike të lidhur me zhvillimet e hapësirës kibernetike në Shqipëri dhe harmonizimin me legjislacionin ndërkombëtar, me qëllim që ai të ngelet i përshtatshëm dhe efektiv. Për të nxitur përdorimin e nënshkrimit elektronik të kualifikuar në transaksionet elektronike janë në proces këto iniciativa:

- Hartimi i draftligjit për përdorimin e identifikimit elektronik të sigurt, vulave elektronike në shërbimet e qeverisjes elektronike; me qëllim garantimin e identitetit në botën virtuale qoftë ky për personat fizik dhe ata juridik. Aktualisht draftligji “Për identifikimin elektronik dhe shërbimet e besuara” është në proces konsultimi në Kuvend. Ndërkohë është gati rregullorja e harmonizuar me direktivën evropiane 910/2014 për zbatimin e ligjit, e cila pritet të miratohet me vendim të Këshilit të Ministrave pas miratimit të draftligjit. Kjo paketë ligjore pritet të rrisë besimin në ambientin online me qëllim zhvillimin ekonomik dhe social, duke rritur besimin mungesa e të cilit deri më sot ka bërë që të ketë pasiguri ligjore e cila i bën konsumatorët, bizneset dhe autoritetet publike të hezitojnë në kryerjen e transaksioneve online.

- Do të futet përdorimi sa më i gjerë i certifikatave për faqe interneti dhe web servera për të garantuar identitetin e sigurt të faqeve të institucioneve publike dhe kompanive të tjera private të cilat ofrojnë shërbime elektronike në bashkëveprim të institucioneve publike ndaj qytetarëve, apo ndaj biznesit.



b) Urdhërimi/detyrimi i kryerjes së auditimit periodik dhe vlerësimit të përshtatshmërisë dhe efektivitetit të sigurisë së sistemeve të informacionit në përputhje me bazën ligjore dhe rregullatore në fuqi. Kjo, për të plotësuar legjislacionin aktualisht në fuqi¹¹ që parashikon auditimin e databazave shtetërore duke lënë jashtë spektrit të veprimit sistemet në tërësi.

c) Zbatimi i procedurave të qarta sipas të cilave institucionet shtetërore të cilat ofrojnë e - shërbime për qytetarin, biznesin, apo për ndërveprim midis institucioneve do të aksesojnë bazat e të dhënave shtetërore me qëllim ndërveprimin dhe përmirësimin e cilësisë së shërbimit për përfituesit.

d) Forcimi i institucioneve dhe rritja e sigurisë në administratën shtetërore, duke aplikuar procedura dhe kërkesa bazë të gjithëpranuara.

Forcimi i kuadrit institucional

a) Zbatimi i procedurave për mbrojtjen e të dhënave personale të qytetarëve në marrjen e e - shërbimeve.

b) Edukimi dhe ndërgjegjësimi i aktorëve në sektorin publik dhe privat lidhur me kuadrin ligjor dhe rregullativ në fuqi.

c) Krijimi i një sistemi raportues të unifikuar për individët dhe bizneset mbi raportimin e krimit kibernetik në mënyrë që të merren masat e nevojshme, si dhe institucionet e forcimit të ligjit të mund të përcaktojnë shkallën sesa krimi kibernetik në Shqipëri ndikon tek individët dhe në ekonomi.

d) Vlerësimi i krijimit të strukturave të nevojshme respektive pranë institucioneve të tjera të administratës publike. Forcimi dhe mbështetja për rritjen e kapaciteteve në fushën e sigurisë kibernetike do të jetë një proces i vazhdueshëm në mënyrë që shteti të shërbejë si model në sigurinë kibernetike.

e) Përcaktimi i qartë i strukturave dhe proceseve të cilat do të sigurojnë koordinimin në nivel politiko-strategjik dhe në nivel operacional duke përfshirë të gjithë aktorët në sektorin publik apo privat.

Rritja e ndërgjegjësimit për sigurinë kibernetike

Botërisht vlerësohet se shumica e sulmeve kibernetike kanë sukses si pasojë e keqkonfigurimit apo mos zbatimit të masave minimale të mbrojtjes nga përdoruesit e TIK-ut.

a) Qeveria do të ndërmarrë iniciativa dhe hartojë programe për edukimin dhe ndërgjegjësimin e përdoruesve të TIK-ut. Këto programe do të përfshijnë të gjithë nivelet e administratës publike, si: specialistët IT, administratorët e sistemeve dhe TIK etj. Ky proces do të garantojë përdorimin, ngritjen dhe ofrimin e shërbimeve dixhitale të administratës në mënyrë të sigurt dhe të besueshme.

b) Shpërndarja dhe publikimi i informacionit mbi rreziqet e hapësirës kibernetike, nxjerrja e udhëzimeve dhe këshillave për një siguri minimale do të jetë një proces i vazhdueshëm nëpërmjet të cilit do të synohet të rritet ndërgjegjësimi dhe siguria e përdoruesve të thjeshtë. Përveç publikimit të tyre në faqet zyrtare të internetit të institucioneve të specializuara do të bashkëpunohet në mënyrë të ngushtë me medien për të siguruar një informim sa më të gjerë dhe të shpejtë të publikut.

c) Vlerësim për futjen e programeve edukative në sistemin arsimor parauniversitar dhe zhvillimi i fushatave të informimit.

d) Bashkëpunimi me sektorin privat si një nga sektorët më të prekshëm nga sulmet kibernetike do të forcohet nëpërmjet marrjes të iniciativave dhe projekteve të përbashkëta. Rritja e ndërgjegjësimit dhe zbatimi i kërkesave minimale të sigurisë do të zbatohet edhe për këtë sektor. Në mënyrë të veçantë ky bashkëpunim do të rritet me:

- Ofruesit e shërbimit të internetit, si portat hyrëse të hapësirës kibernetike në vend. Përmes ndërtimit të besimit të ndërsjellë, bashkëpunimi i ngushtë me ta në baza vullnetare do të rrisë efektivitetin e trajtimit të incidenteve kibernetike duke shkurtuar kohën e përgjigjes; si dhe për të vënë në zbatim masat për bllokimin e aksesit ndaj faqeve të internetit me përmbajtje të paligjshme.

- Shoqërinë civile, për të adresuar çështjet e sigurisë së fëmijëve në internet.

¹¹ Ligj nr. 10325, datë 23.9.2010, “Për bazat e të dhënave shtetërore” dhe vendimit të Këshillit të Ministrave nr. 945, datë 2.11.2012, “Për miratimin e rregullores “Administrimi i Sistemit të Bazave të të Dhënave Shtetërore””.



- Akademinë, për të hapur programe studimi të specializuara në siguri kibernetike e për të ngritur fonde duke shfrytëzuar mundësitë si Horizon 2020.

- Sektorin bankar, si një nga sektorët me fjalën e fundit të teknologjisë në drejtim të sigurisë. Përmes komitetit të tyre të sigurisë, ata do të jenë palë në çdo iniciativë ligjore dhe teknike në këtë fushë; si dhe për shkëmbimin e informacionit mbi dobësitë e produkteve dhe teknologjive të TIK, llojet e reja të sulmeve, institucionalizimin e marrëdhënieve, hartimin e planeve të masave dhe veprimeve të koordinuara dhe shkëmbimin e ndërsjellë të informacionit në lidhje me sulmet kibernetike.

Identifikimi dhe mbrojtja e Infrastrukturave Kritike të Informacionit në Shqipëri

Zhvillimi i teknologjisë dhe integrimi i vazhdueshëm i sistemeve bën që disa sisteme të kthehen në jetike për funksionimin e shoqërisë dixhitale duke i konsideruar ato si infrastruktura kritike.

a) Krijimi i procedurave dhe proceseve të nevojshme për identifikimin, inventarizimin dhe garantimin e sigurisë të tyre. Krijimi dhe implementimi i procedurave dhe kërkesave minimale të sigurisë për këto sisteme do të jetë detyruese.

b) Për shkak se këto sisteme nuk janë vetëm shtetërore, por në të shumtën e rasteve i përkasin sektorit privat, në mënyrë të vazhdueshme do të garantohet siguria bazë e këtyre sistemeve. Lidhur me këtë objektiv një aspekt tjetër mjaft i rëndësishëm përveç mbrojtjes së këtyre sistemeve kritike është “aftësia ripërtëritëse” (*resilience*), e cila mundëson garantimin e vazhdueshmërisë së biznesit në rastet e ndodhjes së forcave madhore apo të sulmeve të ndryshme kibernetike. Mbrojtja dhe aftësia ripërtëritëse e infrastrukturave kritike, si dhe inkurajimi i operatorëve që i zotërojnë ato për implementimin e një arkitekture sigurie të plotë (përfshirë menaxhimin e riskut dhe të emergjencave) do të garantojë efektivitetin, besueshmërinë dhe vazhdueshmërinë e shërbimeve të ofruara prej tyre.

c) Përcaktimi i bazës ligjore/rregullative mbi të cilën operatorët e infrastrukturave kritike do të duhet të raportojnë mbi incidentet e rënda kibernetike. Për çdo rast (të evidentuar ose jo) si krim kibernetik duhet të bëhet analiza e tij, shkaqet e ndodhjes dhe nxjerrja e detyrave që duhet të reflektohen në akte ligjore apo rregullore e procedura për eliminimin e përsëritjes së rastit.

Krijimi dhe implementimi i kërkesave minimale të sigurisë kibernetike

Rritja e sigurisë së pari në administratën shtetërore, rritja e përdorimit të sistemeve TIK në administratën shtetërore por dhe garantimi i sigurisë të tyre është një nga prioritetet e këtij Dokumenti.

a) Standarde, udhëzime dhe procedura të bazuara në praktikat më të mira ndërkombëtare duhet të përshtaten dhe miratohen për t'u zbatuar në administratën shtetërore.

b) Krijimi dhe miratimi i procedurave të analizës të rrezikut të sigurisë për sistemet e përdorura dhe shërbimet elektronike të ofruara nga institucionet është prioritet. Analiza e rrezikut do të jetë një proces i vazhdueshëm dhe do të kryhet në mënyrë periodike. Zbatimi i tyre do të jetë një nga elementet kyçe për rritjen e nivelit të sigurisë kibernetike.

c) Zhvillimi i mëtejshëm i procedurave për koordinimin e investimeve me synim analizimin e sigurisë dhe harmonizimin e projekteve që në fazat e projektimit.

d) Do të identifikohen sistemet e rëndësishme në administratën shtetërore dhe institucionet do të investojnë në *hardware* dhe *software* të automatizuara si masa proaktive dhe reaktive për të siguruar këto sisteme që administrojnë.

e) Do të ngrihen BCC (*Business Continuity Center*) dhe DRC (*Disaster Recovery Center*) për rrjetet/sistemet shtetërore.

f) Do të ngrihet një sistem monitorimi, i cili do t'i njoftonte në kohë institucionet për rreziqet kibernetike që u kanosen duke monitoruar 24/7 nyjet më të rëndësishme, trafikun dhe eventet që ndodhin në sistem për të mundësuar edhe nxjerrjen e konkluzioneve nga logg-et që ruhen, pa ndërhyrë apo monitoruar përmbajtjen.

Forcimi i partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit

Koordinimi dhe bashkëpunimi i të gjithë aktorëve është elementi bazë për garantimin e suksesit. Për shkak të dinamikës dhe shpejtësisë me të cilën zhvillohet TIK bashkëpunimi me sektorin privat do të forcohet. Vetëm nëpërmjet një bashkëpunimi të ngushtë mund të rritet siguria dhe zhvillimi i TIK në administratën shtetërore në koherencë me zhvillimet dhe trendin e teknologjisë.



a) Rritja e bashkëpunimit dhe koordinimit ndërmjet institucioneve shtetërore do të forcohet për të garantuar ndërveprimin dhe koordinimin në forcimin e sigurisë dhe minimizimin e dëmeve nga sulmet kibernetike.

b) Shqipëria mbështet dhe do të jetë pjesë e iniciativave ndërkombëtare të cilat synojnë rritjen dhe forcimin e sigurisë. Në mënyrë të veçantë do të forcohet bashkëpunimi me NATO-n dhe BE-në duke u bërë pjesë aktive e iniciativave të përbashkëta për sigurinë kibernetike. Anëtarësimi i Shqipërisë në organizmat dhe shoqatat e sigurisë kibernetike të njohura ndërkombëtare dhe rritja e bashkëpunimit është prioritet.

Rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike

Në afatshkurtër dhe afatmesëm do të realizohen aktivitete me qëllim ngritjen e kapaciteteve të burimeve njerëzore të nevojshme në fushën e sigurisë kibernetike. Do të krijohen rregullore për të përfshirë konceptin e sigurisë kibernetike në programet e shkollave fillore, shkollave të mesme, dhe të institucioneve të arsimit të lartë. Do të diskutohen gjithashtu hapat e auditimit mbi sigurinë kibernetike në proceset e auditimit të brendshëm të organizatave.

a) Në kuadër të forcimit të institucioneve, do të rriten kapacitetet teknike të burimeve njerëzore. Kjo do të bëhet përmes programeve të zgjedhura të trajnimeve të cilat do të synojnë aftësimin e pjesëmarrësve në parandalimin e sulmeve, minimizimin e dëmeve, dhënien e përgjigjes efektive ndaj incidenteve të sigurisë së informacionit.

b) Pjesëmarrja aktive në konferenca ndërkombëtare, takime, seminare dhe ushtrime që kanë të bëjnë me sigurinë kibernetike. Shkëmbimi i informacioneve, analizave, eksperiencave, krijimi i projekteve të përbashkëta, vlerësimi i teknologjive dhe sistemeve të sigurisë shihen jo vetëm si një mundësi për rritjen e sigurisë kibernetike në institucionet publike, por dhe si një investim për zhvillimin dhe rritjen e kapaciteteve të brezave pasardhës.

Analiza SWOT (*strength, weakness, opportunities, threats*)

Për hartimin e këtij dokumenti është hartuar një analizë SWOT që lidhet me pikat e forta, të dobëta, mundësitë dhe kërcënimet që mund të ndikojnë në mosrealizimin e suksesshëm të saj.

Fortësitë	Dobësitë
a) Përjasje që synon të forcojë bashkëpunimin ndërmjet Qeverisë me operatorët e Infrastrukturave Kritike të Informacionit b) Institucione të angazhuara për implementimin e Dokumentit të Politikave, si dhe institucione gjithmonë më të ndërgjegjësuar për rreziqet që i kanosen hapësirës kibernetike; c) Plan veprimi i strukturuar me mekanizma të qartë që do të lejojnë monitorim të zbatimit të këtij dokumenti.	a) Mungesë historiku në fushën e sigurisë kibernetike: i) Mungesë strategjie në nivel kombëtar në këtë fushë deri më tani; ii) Mungesë kuadri rregullator. b) Nevojë për investime madhore për të arritur nivele të krahasueshme me rajonin dhe BE-në, deri më tani siguria nuk theksohej që në fazat fillestare të ngritjes së infrastrukturave të TIK-ut; c) Kuadri ekzistues ligjor dhe institucional ka nevojë për t'u plotësuar d) Mungesë e profesionistëve të specializuar dhe të certifikuar për sigurinë kibernetike; e) Nivel i ulët i kulturës së navigimit të sigurt në internet në popullatë.
Mundësitë	Kërcënimet
a) Janë ngritur tashmë struktura përgjegjëse në hallka të ndryshme të procesit të menaxhimit të sigurisë kibernetike; b) Akses në praktikat më të mira ndërkombëtare dhe mundësi për t'u mbështetur në dokumente strategjike	a) Mungesë koordinimi dhe vullneti për të përmbushur detyrimet; b) Fragmentizimi i burimeve dhe mbivendosja e investimeve.



rajonale, si dhe të partnerëve evropianë e të NATO-s;
c) Investimet nga ana e Qeverisë në fushën e TIK janë gjithnjë e në rritje si në pikëpamje të teknologjisë ashtu edhe të burimeve njerëzore.

Llogaridhënia, monitorimi dhe analiza vlerësuese

Formimi i sigurisë kibernetike në kushtet e një teknologjie informacioni që ndryshon dita ditës kërkon vëmendje të veçantë nga ana e institucioneve publike. Ato duhet të përcaktojnë kushtet e nevojshme dhe mënyrat për të përshpejtuar procesin e përfshirjes aktive të sektorit privat dhe publik për të diskutuar politikat e këtij Dokumenti, si dhe zbatimin me efikasitet të tyre.

Institucionet Qeveritare luajnë një rol udhëheqës në termat e:

1. Plotësimi të kuadrit ligjor në fushën e sigurisë kibernetike;
2. Identifikimin dhe mbrojtjen e Infrastrukturave Kritike të Informacionit (CIIP);
3. Krijimin dhe implementimin e kërkesave bazë të sigurisë kibernetike;
4. Shtimin i investimeve për rritjen e sigurisë në rrjetet/sistemet shtetërore;
5. Forcimin e partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit;
6. Rritjen e ndërgjegjësimi për sigurinë kibernetike;
7. Rritjen e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike.

Institucionet qeveritare duhet të krijojnë parakushtet, si dhe duhet të nxisin sektorin privat, OJQ-të dhe veçanërisht operatorët e infrastrukturave kritike të informacionit, që:

- të marrin pjesë në procesin e përmirësimit të kuadrit ligjor në fushën e sigurisë kibernetike;
- të jenë aktiv në procesin e identifikimit të infrastrukturave kritike të informacionit;
- t'i kushtojnë një rëndësi të veçantë rritjes së kapaciteteve njerëzore;
- marrin pjesë aktivisht në përcaktimin e kërkesave minimale të sigurisë kibernetike;
- pjesëmarrjen në takimet me përfaqësues të institucioneve shtetërore dhe private për të zgjidhur çështje të rëndësishme;
- paraqitjen e projekteve dhe pjesëmarrjen në diskutimet publike mbi legjislacionin;
- të marrin pjesë në partneritete publik-privat;
- rritjen e pjesëmarrjes në monitorimin e rezultateve të këtij dokumenti politikash.

Ky dokument politikash do të monitorohet nga Grupi Ndërinstitucional i Punës për Hartimin e “Dokumentit të Politikave për Sigurinë Kibernetike”, i ngritur me urdhër të Kryeministrit nr. 120, datë 20.3.2014, ministri përgjegjës për Administratën Publike dhe Inovacionin, Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT), si dhe Departamenti i Programimit të Zhvillimit, Financimeve dhe Ndihmës së Huaj pranë Këshillit të Ministrave.

Parakushtet për zbatimin efikas dhe me sukses të “Dokumentit të Politikave për Sigurinë Kibernetike 2015–2017”, përfshijnë:

- Konsensusin e përgjithshëm dhe vullnetin e mirë për të zbatuar objektivat dhe aktivitetet e propozuara;
- Promovimi i “Dokumentit të Politikave për Sigurinë Kibernetike 2015–2017”, si dhe objektivate të tij, si ndaj sektorit publik, privat dhe qytetarëve;
- Një sistem i monitorimit dhe vlerësimit efikas për të kontrolluar nëse objektivat e përcaktuara në Dokumentin e Politikave janë realizuar;
- Nxitja e bashkëpunimit ndërmjet autoriteteve shtetërore, si dhe njohja e vazhdueshme me praktikën më të mirë të rajonit.

Zbatimi i këtij dokumenti politikash do të bazohet në përdorimin e një numri treguesish të lidhur me inputet, proceset, produktet dhe efektet e planit të veprimit. Treguesit do të vlerësohen në mënyrë periodike nga institucionet publike sipas ndarjes së punës dhe sferës së tyre të juridiksionit në fushën e sigurisë kibernetike. Treguesit do të mblidhen nga ALCIRT-ja përkatësisht sipas treguesve të



paracaktuar në këtë dokument për përmbushjen e çdo politike në bashkëpunim me institucionet e ndryshme publike. Bazuar në këto tregues ministri përgjegjës për Administratën Publike dhe Inovacionin do të prodhojë raporte vjetore të ecurisë së dokumentit të politikave, të cilat do të jetë publike.

Ngritja e një sistemi monitorimi dhe vlerësimi efektiv do të mbështetet nga aktivitete të forcimit të kapaciteteve njerëzore dhe strukturore, si dhe investim në infrastrukturën e TIK-ut më të sigurt. Informimi i publikut, si dhe monitorimi i zbatimit të dokumentit të politikave dhe rezultateve të tij nga shoqëria civile, si dhe operatorët e sektorit privat do të përbëjnë gjithashtu një nga elementet bazë të sistemit të monitorimit dhe llogaridhënies.

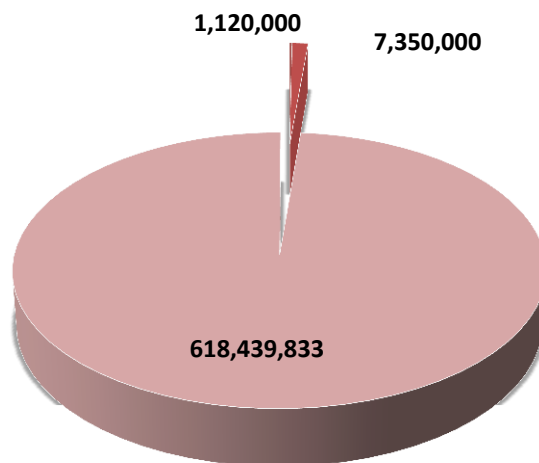
Financimi i Dokumentit të Politikave

Përcaktimi i nevojave të financimit të “Dokumentit të Politikave për Sigurinë Kibernetike 2015–2017” u realizua nëpërmjet procesit të vlerësimit të kostove potenciale të nevojshme, nga secili institucion i përfshirë në këtë Dokument. Çdo institucion ka përgjegjësinë kryesore në realizimin e aktiviteteve të parashikuara në planin e veprimit që shoqëron këtë Dokument.

Fondet e vlerësuara të nevojshme për zbatimin e aktiviteteve të detajuara në planin e veprimit të këtij Dokumenti gjatë periudhës kohore 2015–2017 parashikohet të jenë 626,909,833 lekë.

Objektivat strategjikë të Dokumentit	Kostot e vlerësuara
OBJ.1. Plotësimi i kuadrit ligjor në fushën e sigurisë kibernetike	Kosto të funksionimit të institucioneve
OBJ.2. Forcimi i kuadrit institucional	Kosto të funksionimit të institucioneve
OBJ.3. Rritja e ndërgjegjësimit për sigurinë kibernetike	1,120,000 ALL
OBJ.4. Identifikimi dhe mbrojtja e Infrastrukturave Kritike të Informacionit në Shqipëri	Kosto të funksionimit të institucioneve
OBJ.5. Krijimi dhe implementimi i kërkesave minimale të sigurisë kibernetike	Kosto të funksionimit të institucioneve dhe 618,439,833 ALL
OBJ.6. Forcimi i partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit	Nuk janë vlerësuar kosto
OBJ. 7. Rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike	7,350,000 ALL

Kostimi i Objektivave Strategjike (ne leke)



U. 2. Rritja e ndërgjegjësimit për sigurinë kibernetike

U. 3. Rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike

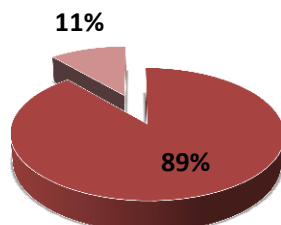
Krijimi dhe implementimi i kërkesave minimale të sigurisë kibernetike

Duhet theksuar se nevojat për financimin e zbatimit të Dokumentit të Politikave janë llogaritur për zbatimin e aktiviteteve për periudhën 2015–2017, por duhet theksuar se në tërësinë e aktiviteteve të parashikuara, një pjesë e tyre, përkatësisht aktivitetet që i shërbejnë realizimit të objektivave 1, 2, 4 dhe 6, nuk mund të përcaktohen në këtë fazë, pasi ata janë aktivitete, fillimi i të cilëve varet tërësisht nga përfundimi i aktiviteteve paraprake ku përmendim: plotësimi i kuadrit ligjor, varësi nga përfundimi i punës së ndonjë Grupi Ndërinstitucional Pune për këtë qëllim ose sepse këto aktivitete realizohen me punën e punonjësve të institucioneve dhe janë pjesë e detyrave të tyre të kohëpaskohëshme etj. Burimi i financimit për këtë Dokument është Buxheti i Shtetit (me PBA). Kosto e vetme e pambuluar nga PBA-ja dhe/ose donatorët është vlera prej 70,000,000 lekësh, e parashikuar për “Krijimin e infrastrukturës për sistemin e monitorimit dhe atë të mbrojtjes (ISMS)”, pra rreth 11,1%, i përcaktuar si aktivitet për plotësimin e objektivit strategjik të pestë.



Burimi i Financimit

■ Financim i mbuluar me PBA ■ Hendeku financiar



Megjithatë, kostimi i “Dokumentit të Politikave për Sigurinë Kibernetike 2015–2017” do të jetë objekt rishikimi vjetor njëloj, si edhe vetë Dokumenti, në mënyrë që të reflektohet qartë plani i financimeve dhe realizimi faktik i tyre.

INDIKATORËT E “DOKUMENTIT TË POLITIKAVE PËR SIGURINË KIBERNETIKE 2015–2017”

INDIKATORËT	BAZAMENTI	BURIMI I VERIFIKIMIT	AFATI I REALIZIMIT	SYNIMI 2017	PËRCAKTIMI DHE QËLLIMI
Kuadri ligjor në fushën e sigurisë kibernetike dhe krimi kibernetik					
100% e kuadrit rregullator e hartuar dhe e vënë në zbatim	Nuk matet aktualisht.	Në vazhdim do të matet nga MSHIAP/ALCIRT	2016	100%	Akronimi: Ak_sk Përcaktimi: Numri i ligjeve si dhe VKM-ve, udhëzimeve dhe rregulloreve të dala në zbatim të ligjeve me qëllim plotësimin e kuadrit ligjor në këtë fushë.
100% e kuadrit rregullator e hartuar dhe e vënë në zbatim për certifikimin elektronik, ne mbështetje të Direktive Evropiane 1999/93/EC	Të dhënat e vitit 2015, 11 Akte ligjore dhe nenligjore	MSHIAP/AKCE	Ne punim Ligj i ri: “Për identifikimin elektronik dhe shërbimet e besuara”; Rregullore dhe akte të tjera nenligjore në zbatim të ketij ligji (pas miratimit në Parlament)	100%	Akronimi: Ak_ce Përcaktimi: Numri i ligjeve si dhe VKM-ve, udhëzimeve dhe rregulloreve të dala në zbatim të ligjit “Për Nënshkrimin Elektronik”.
Krime kibernetike të evidentuara, në zbatim të Kodit Penal të Republikës së Shqipërisë	Të dhënat e vitit 2013, 108 krime	Policia e Shtetit	Tendencë në ulje.	Tendencë në ulje.	Akronimi: N_kke Përcaktimi: Numri i krimeve kibernetike të evidentuara, në zbatim të Kodit Penal të Republikës së Shqipërisë nga Policia e Shtetit.
Krime kibernetike të zbuluara	Të dhënat e vitit 2013, 63 krime	Policia e Shtetit	Tendencë në rritje.	Tendencë në rritje.	Akronimi: N_kkz Përcaktimi: Numri i krimeve kibernetike të zbuluara, në zbatim të Kodit Penal të Republikës së Shqipërisë.
Identifikimi dhe mbrojtja e Infrastruktura Kritike të Informacionit					
70% e kuadrit rregullator për Infrastruktura Kritike të Informacionit e hartuar dhe e vënë në zbatim	Nuk matet aktualisht.	Në vazhdim do të matet nga ALCIRT.	2016	70%	Akronimi: Ak_cii Përcaktimi: Numri i akteve nenligjore me qëllim identifikimin nominal të infrastrukture kritike të informacionit në RSH.
80% e Infrastruktura Kritike të Informacionit të identifikuar	Nuk matet aktualisht.	Në vazhdim do të matet nga ALCIRT.	2016	100%	Akronimi: N_cii Përcaktimi: Numri i infrastrukture kritike të informacionit të identifikuar.
Krijimi dhe implementimi i kërkesave minimale të sigurisë					
Hartimi e miratimi i kërkesave minimale të sigurisë për administratën	Nuk matet aktualisht.	ALCIRT	2016	100%	Akronimi: K_msk Përcaktimi: Kërkesat minimale të hartuara e të miratuara, gati për tu zbatuar nga administrata publike.
Hartimi e miratimi i masave të sigurisë për bazat e të dhënave shtetërore	Nuk matet aktualisht.	ALCIRT, AKSHI	2016	100%	Akronimi: K_msbd Përcaktimi: Tërësia e masave të sigurisë të hartuara e të miratuara për çdo klasë sigurie të bazave të të dhënave shtetërore.
Miratim të projekteve TIK të lidhura me sigurinë	Të dhënat e vitit 2014	Në vazhdim do të matet nga AKSHI.	Tendencë në rritje.	Tendencë në rritje.	Akronimi: N_ptik Përcaktimi: Numri i projekteve TIK që synojnë të rrisin sigurinë kibernetike,



					të miratuara nga AKSHI. Numri i projekte të tilla që miratohen nga totali i propozuar. (% dhe si numër).
Numri i certifikatave elektronike të kualifikuara lëshuar ndaj funksionarëve të administratës shtetërore	Të dhënat e vitit 2014, muaji Maj 30 funksionare publik	AKCE/AKSHI/	Tendencë në rritje.	Tendencë në rritje.	Akronimi: Np_ne Përcaktimi: Numri i punonjësve të administratës që janë pajisur me usb token dhe certifikatë elektronike nga AKSHI.
Numri i certifikatave elektronike të kualifikuara lëshuar ndaj qytetarëve.	Të dhënat e vitit 2014, muaji Maj 181.000 qytetarë	AKCE / ALEAT shpk	Tendencë në rritje.	Tendencë në rritje.	Akronimi: Npq_ne Përcaktimi: Numri i qytetarëve që kanë aktivizuar autentikimin dhe certifikatë elektronike në kartën ID ofruar nga ALEAT.
Përdorues govnet të cilëve u ofrohet menaxhim i përqendruar antivirusi	Të dhënat e 2014.	Në vazhdim do të matet nga AKSHI.	Tendencë në rritje.	Tendencë në rritje.	Akronimi: N_a Përcaktimi: Sa është numri i përdoruesve govnet të cilëve u ofrohet menaxhim i përqendruar antivirusi nga AKSHI.
Incidente kompjuterike të raportuara	Të dhënat e 2014, 11 incidente.	ALCIRT	Tendencë në rritje.	Tendencë në rritje.	Akronimi: N_ik Përcaktimi: Numri i incidenteve kompjuterike të raportuara pranë ALCIRT
Incidente kompjuterike të trajtuara	Të dhënat e 2014, 11 incidente, 11 incidente te asistuar.	Çdo subjekt raportues dhe ALCIRT	Tendencë në rritje.	Tendencë në rritje.	Akronimi: N_ikt Përcaktimi: Numri i incidenteve kompjuterike të trajtuara nga subjekti raportues në bashkëpunim me ALCIRT
Niveli i njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike					
80% e punonjësve TI të administratës publike të trajnuar	Të dhënat e vitit 2014, 40 nëpunës TI	ASPA dhe ALCIRT	2016	80%	Akronimi: N_pitb Përcaktimi: Numri i punonjësve IT të administratës publike të trajnuar me modulin bazë të sigurisë kibernetike.
80% e punonjësve TI të administratës publike të trajnuar	Të dhënat e vitit 2014, 10 nëpunës TI	ASPA dhe ALCIRT	2016	80%	Akronimi: N_pitav Përcaktimi: Numri i punonjësve IT të administratës publike të trajnuar me modulin e avancuar të sigurisë kibernetike.



PLANI I VEPRIMIT “DOKUMENTI I POLITIKAVE PER SIGURINE KIBERNETIKE 2015 – 2017”

	Aktivitet	Përshkrimi i aktivitetit	Institucioni/et përgjegjëse	Afatet për implementim	Kostot në Lekë		
					PBA	Donatorë	Të tjerë
	Hartimi i planit të veprimit të Dokumentit të Politikave për Sigurinë Kibernetike	Hartimi i Planit të veprimit, i cili do t'i hapë rrugë iniciativave në fushën e sigurisë kompjuterike. Ky plan do të bashkëngjitet për miratim Dokumentit të Politikave të Sigurisë Kompjuterike.	ALCIRT, GNP	2014 – në vijim			
OBJ. 1	Plotësimi i kuadrit ligjor/rregullator në fushën për sigurinë kibernetike	1. Hartimi i draft ligjit final për sigurinë kibernetike	1. ALCIRT, MIAP, AKSHI, AKCE, MD, DSIK, MM, MPB (Me mbështetje nga TAIEX)	1. 2014 - 2015	1. Me mbështetje të TAIEX		



OBJ. 2	Rritja e ndërgjegjësimit për sigurinë kibernetike	Ndërgjegjësimi ndaj rrezikut të krimit kibernetik: 1. Krijimi i nje portali ndërgjegjesimi me fokus sigurinë kompjuterike, femijet ne internet, biznesin, keshilla sigurie dhe artikuj. 2. Fushate ndërgjegjesimi ne Fakultetet e drejtimit TIK ne formen e leksioneve te hapura, seminareve. Fushate ndërgjegjesimi me e gjere (jo vetem me studentet; psh. Muaji i ndërgjegjesimit per sigurine kompjuterike) 3. Ndergjegjesim permes materialeve informuese (fletëpalosje, broshura, poster); 4. Organizimi i konkurseve me	1. ALCIRT (Permbajtja do te pasurohet nga institucionet e meposhtme: ALCIRT, KDIMDP, IZHA, AKCE, AKSHI, AKEP, si dhe sektori privat). <i>--Portali cyberalbania.al i ndërgjegjesimit per sigurine kompjuterike (ALCIRT, 260,000 ALL)</i> 2. ALCIRT, AKCE, IDP si dhe institucione publike e private te ftuara sipas rastit. <i>--Konference me sektorin e IT-se mbi prezantimin e Udhëzuesit "Për mbrojtjen e të dhënave personale në shërbimet cloud computing" (IDP, 60,000 ALL)</i> <i>--Muaji i ndërgjegjesimit per sigurine kompjuterike (ALCIRT, 800,000 ALL)</i> 3. MIAP, MAS, ALCIRT, IDP	1. Qershor 2014, ne vijim ne perditësim 2. Maj 2014- Dhjetor 2015 3. Korrik 2014- ne vijim 4. Konkursi i pare i ketij lloji ne tremujorin e fundit te 2015.	1. 260,000 2. Kosto infrastruktur e per tu vleresuar; 860,000 dhe te tjera pa kosto 3. Per tu vleresuar me kohen (materiale konsumi) 4. Kostot per tu vleresuar.		
-------------------	---	--	---	--	---	--	--



		fokus sigurine per evidentimin e talenteve te reja ne kete fushe.	--Kater aktivite per mbrojtjen e femijeve Online: Konferenca Vjetore Kombetare "Siguria e Femijeve ne Internet" Fushate ndergjegjesuese ne 3 DAR per mbrojtjen e femijeve online. Organizimi i trajnimeve per Sigurine kompjuterike per specialistet TIK te DAR/ZA-ve. Trajnimi i mesuesve TIK te Drejtorive Rajonale dhe Zyrave Arsimore perkatese nga personeli TIK i DAR/ZA ne sistemin kaskade Krijimi i Posterave Sensibilizues ne te gjitha shkollat e DAR/ZA-ve. Pergatitja e Broshures Elektronike dhe e printuar per DAR/ZA-te.				
			4. ALCIRT, AKSHI, Protik				
OBJ. 3	Rritja e nivelit te njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë	1. Organizimi i trajnimeve për profesionistët IT te administrates	1. ALCIRT, ASPA --4 trajnime baze per sigurine ne periudhen Shtator-Dhjetor, si dhe 10 cikle trajnimi gjate vitit	1. Shtator 2014 – ne vijim 2. 2014 (ne kurrikulat pilot) 3. 2015 – 2016 4. 2015 - 2017	1. 1,350,000 (per vitin 2014-2015) 2. Pa kosto		



	kibernetike	publike 2. Përfshirja në kurrikula e çështjeve të “cyber security” në arsimin parauniversitar për një internet me të sigurtë për fëmijet e adoleshentët si përdorues të TIK, pilotimi në klasën e 6-shtë gjatë vitit akademik 2014-2015. 3. Studime pasuniversitare (dege masteri) të specializuara drejt sigurisë kibernetike 4. Rritja e kapaciteteve për stafin përgjegjës për sigurinë	2015 (300,000 ALL + 1,050,000 ALL) 2. ALCIRT, IZHA (MAS), IDP. -- <i>Integrimi i Tik-ut në kurrikulën e arsimit parauniversitar (k-12) duke filluar që nga klasa e IV-të e arsimit bazë dhe në vazhdim në të gjitha klasat e arsimit parauniversitar.</i> 3. MIAP, ALCIRT, Universitetet publike me drejtim TIK. 4. ALCIRT, DPD, AKSHI, Ministrinë e Linjes -- <i>Ngritje kapaciteti të stafit ALCIRT (5,000,000 ALL)</i> -- <i>Ngritje kapaciteti të stafit DPD (1,000,000 ALL)</i> -- <i>Te tjera pa kosto nga bashkepunimet</i>		shtese (kosto të funksionimit të IZHA) 3. Për tu vlerësuar. 4. 6,000,000 dhe të tjera pa kosto në kuadër të bashkepunimeve me strukturë jashtë vendit.		
OBJ. 4	Identifikimi i infrastrukturave kritike (CIIP)	Identifikimi i sistemeve të informacionit që sigurojnë funksionimin e shërbimeve jetike të shoqërisë.	ALCIRT, AKSHI, institucionet publike dhe grupet e interesit.	2015	Pa kosto identifikimi i CII (me Grup Pune, me tej masa dhe shpërndarja		



					e koston se mbrojtjes per tu vleresuar ne procesin e identifikimi)		
OBJ. 5	Implementimi i nje kerkesave minimale te sigurise	1. Hartimi/implementimi i kerkesave minimale te sigurise per administraten publike për nivelin e sigurisë së nevojshme në sektorin publik. 2. Procedure per menaxhimin e incidenteve. 3. Monitorimi periodik i tyre.	1. ALCIRT, AKSHI 2. ALCIRT, AKSHI 3. ALCIRT	1. 2015 - 2016 2. 2015 3. Ne vazhdim	1. Pa kosto hartimi, aplikuar per mbeshtetje nga donatore. 2. Kosto te funksionimit te ALCIRT. 3. Kosto te funksionimit te ALCIRT.		
OBJ. 6	Shtimi i infrastrukturave te sigurise ne rrjetet/sistemet shteterore	1. Investime në hardware dhe software të automatizuara si masa proaktive dhe reaktive për të siguruar sistemet që administrojnë. 2. Ngritja e BCC-ve (Business Continuity Center) dhe DRC-ve (Disaster Recovery Center) për rrjetet/sistemet	1. ALCIRT, AKSHI, SHISH, Ministria e Financave (DPT, DPD), MZHETS --Ngritja e portalit per bllokimin e faqeve te internetit me permbajtje te paligjshme (19,500,000 ALL) ALCIRT --Realizimin e Penetration Test (46,500,000ALL) ALCIRT -- Rritja e Sigurisë në rrjetin qeveritar GovNet	1. 2015 - 2017 2. 2015 – 3. 2016 - 2017	1. 548,439,833 2. Kostot per tu vleresuar gjate kohes		3. 70,000,000 (pa mbuluar)



		shtetërore. 3. Krijimi i Infrastruktues per sistemin e monitorimit dhe ate te mbrojtjes (ISMS)	<i>dhe qendrën e të dhënave qeveritare (80,820,833ALL) AKSHI -- Blerja e System Management Solution (Anti-malware, controls, mobile security & MDM, Automatic vulnerability scanning & patch distribution, protection for Web gateway, email & collaboration) dhe Penetration Test (12,400,000ALL) DPT --Upgrade i sistemit Checkpoint Liçensa backup;; Check Point për HA Firewall-in e Internetit;; Sherbim për Penetration testing i sigurisë së rrjetit/sistemeve TI (7,530,000ALL) DPD --Infrastruktura sigurie (381,689,000ALL) SHISH</i> 2. AKSHI dhe institucione te tjera 3. ALCIRT dhe institucione te tjera				
--	--	--	---	--	--	--	--



OBJ. 7	Forcimi i partneritetit me struktura te tjera pergjegjese te fushes brenda dhe jashte vendit	Forcimi i partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit si: NATO; ENISA, CERT-et e huaja; CERT-et sektoriale (Banka, ISP, Telekomunikacioni, Universitete). 1. Pjesemarrje periodike aktive e eksperteve te sigurise ne Cyber Exercises. 2. Nenshkrimi i marrëveshjeve te bashkëpunimit me institucione publike (MAS, Policia e Shtetit, BSH etj) dhe sektorin privat (ISP, Sektori bankar, ICT service/product provider).	1. ALCIRT, AKSHI, SHISH, DPSH 2. ALCIRT	1. 2014 ne vijim 2. 2014 - 2015	Nuk jane vleresuar kosto.		

	Formati 61x86/8
--	-----------------

Shtypshkronja e Qendrës së Botimeve Zyrtare
Tiranë, 2015

Adresa
Bulevardi “Gjergj Fishta”,
pas ish-Ekspozitës “Shqipëria Sot”,
Tel: 042427005, 04 2427006

Çmimi 308 lekë