VENDIM
Nr. 542, datë 25.7.2019

PËR MIRATIMIN E RREGULLORES "PËR SIGURIMIN E INFORMACIONIT TË KLASIFIKUAR QË TRAJTOHET NË SISTEMET E KOMUNIKIMIT DHE TË INFORMACIONIT (SKI)"

Në mbështetje të nenit 100 të Kushtetutës dhe të nenit 31, të ligjit nr. 8457, datë 11.2.1999, "Për informacionin e klasifikuar "Sekret shtetëror"", të ndryshuar, me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI:

1. Miratimin e rregullores "Për sigurimin e informacionit të klasifikuar që trajtohet në sistemet e komunikimit dhe të informacionit (SKI)".
2. Ngarkohen Drejtoria e Sigurimit të Informacionit të Klasifikuar dhe Drejtoria e Shifrës për ngritjen e autoriteteve përkatëse brenda vitit 2020.
3. Institucionet shtetërore, të cilat nuk përmbushin standardet e sigurisë për ngritjen e strukturave të parashikuara në këtë vendim, të marrin masat për arritjen e standardeve brenda vitit 2021.
4. Ministritë, institucionet shtetërore dhe operatorët ekonomikë duhet që, brenda 90 (nëntëdhjetë) ditëve nga hyrja në fuqi e këtij vendimi, të nxjerrin udhëzimet përkatëse për zbatimin e tij.
5. Vendimi nr. 922, datë 19.12.2007, i Këshillit të Ministrave, "Për sigurimin e informacionit të klasifikuar "Sekret shtetëror" që prodhohet, ruhet, përpunohet apo transmetohet në sistemet e komunikimit (INFOSEC)", shfuqizohet.
6. Ngarkohen ministritë, institucionet shtetërore dhe operatorët ekonomikë për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

RREGULLORE
PËR "SIGURIMIN E INFORMACIONIT TË KLASIFIKUAR QË TRAJTOHET NË SISTEMET E KOMUNIKIMIT DHE TË INFORMACIONIT (SKI)"[1]

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Hyrje

1. Institucionet shtetërore dhe operatorët ekonomik/kontraktorët që për nevoja të punës, prodhojnë, ruajnë, përpunojnë, shpërndajnë ose transmetojnë informacion të klasifikuar "Sekret shtetëror", të NATO-s, BE-së, shteteve dhe/ose organizatave të huaja me të cilat RSH-ja ka marrëveshje sigurie nëpërmjet sistemeve të komunikimit dhe informacionit, duhet t'u përmbahen kërkesave të përcaktuara në këtë rregullore.

[1] Referuar "Vendimit të Këshillit të datës 23 Shtator 2013 "Mbi rregullat e sigurisë për mbrojtjen e informacionit të klasifikuar të BE (2013/488 / BE). Nr. CELEX: EUR-Lex- 32013D0488. Nr. Natyral: 2013/488/EU

2. Kjo rregullore zbatohet për sistemet e komunikimit dhe informacionit që trajtojnë ose që do të trajtojnë informacion të klasifikuar "Sekret shtetëror", të NATO-s, BE-së, shteteve dhe / ose organizatave të huaja me të cilat RSH ka marrëveshje sigurie (këtej e tutje referuar si SKI).

3. Me kërkesë të DSIK, institucionet shtetërore dhe operatorët ekonomik/kontraktorët japin informacion në lidhje me zbatimin e masave të sigurisë në sistemet e klasifikuara.

Neni 2
Objekti dhe qëllimi

1. Dispozitat e përcaktuara në këtë rregullore kanë për qëllim garantimin e sigurisë së sistemeve të klasifikuar dhe informacionit të klasifikuar që trajtohet në to.

2. Objekt i kësaj rregulloreje është:

a) Identifikimi i autoriteteve kombëtare të sigurisë së SKI-ve dhe përcaktimi i detyrave kryesore të tyre.

b) Përcaktimi i kërkesave minimale që duhet të implementohen për sigurinë e SKI-ve.

c) Përcaktimi i procedurës për aktivitetet e certifikimit dhe akreditimit të sigurisë së SKI-ve.

Neni 3
Përkufizime

Në këtë rregullore termat e mëposhtëm kanë këto kuptime:

1. "Certifikim i sistemit të komunikimit dhe informacionit" është procesi i vlerësimit, testimit dhe ekzaminimit të masave/ kontrolleve të sigurisë të sistemit, në bazë të standardeve specifike të sigurisë, si dhe identifikimi i dobësive të sistemit dhe përpilimi i planit të masave minimizuese të këtyre dobësive.

2. "Akreditim i sistemit të komunikimit dhe informacionit" është procesi i pranimit të riskut të mbetur, lidhur me vazhdimësinë e operimit të sistemit të komunikimit dhe informacionit dhe autorizimit të tij për të operuar për një kohë të përcaktuar.

3. "Siguria e sistemeve të komunikimit dhe informacionit" është aplikimi i masave të sigurisë për mbrojtjen e informacionit dhe SKI-ve sipas objektivave të sigurisë.

4."Siguria e informacionit" përfshin përcaktimin dhe zbatimin e masave për mbrojtjen e informacionit të klasifikuar që trajtohet në SKI nga humbja aksidentale apo e qëllimshme e konfidencialitetit, integritetit dhe disponueshmërisë, dhe masat për parandalimin, humbjen e integritetit dhe disponueshmërisë së këtyre sistemeve.

5. "Ngjarje e sigurisë" është çdo ngjarje që rezulton ose mund të rezultojë në padisponueshmëri të sistemit ose të komponentëve të tij kryesorë, zbulim të informacionit të klasifikuar, humbje ose ndryshim të padëshiruar të informacionit, shkatërrim ose humbje të pajisjeve ose aseteve.

6. "Emetim elektromagnetik kompromentues" është rrezatimi elektromagnetik i pakontrolluar që mundëson, ekspozimin e pa autorizuar të informacionit të klasifikuar "Sekret shtetëror".

7. "TEMPEST" është studimi dhe kontrolli i emetimeve elektromagnetike komprometuese.

8. "Menaxhimi i riskut" është procesi i identifikimit, analizimit dhe vlerësimit të riskut të sigurisë së informacionit si dhe marrjes së masave për reduktimin e tij brenda një niveli të pranueshëm.

9."Aset" është çdo gjë me vlerë, si pajisje e teknologjisë së informacionit dhe komunikimit, komponent softëare dhe informacioni.

10. Kërcënimet, në terma të përgjithshëm, përcaktohen si mundësi për kompretimin e qëllimshëm ose jo të sigurisë. Në rastin e sigurisë së sistemeve, kompretimet e tilla përfshijnë humbjen e një ose më shumë objektivave të sigurisë së SKI-ve.

11. Dobësitë janë mangësi në fortësinë, plotësinë ose konsistencën e kontrolleve dhe mund të jenë të natyrës teknike, proceduriale ose operacionale.

12. "Risk" probabiliteti që një ngjarje të shfrytëzoj një dobësi duke cënuar objektivat e sigurise.

13. "Risku i mbetur" është risku që mbetet pas implementimit të masave të sigurisë në SKI, duke marrë parasysh që jo të gjithë kërcënimet dhe dobësitë mund të eliminohen apo reduktohen.

14. "Incident i sigurisë së sistemit" është çdo anomali e detektuar që kompromeTon apo ka aftësinë të kompromentojë informacionin ose SKI-të.

15. "Entitet" në kuptim të kësaj rregulloreje përfshin individë, pajisje ose shërbime.

16."Nevoja për njohje" është nevoja për të pasur akses tek informacioni i klasifikuar, në kuadrin e një pozicioni zyrtar dhe me qëllim përmbushjen e një detyre specifike.

17. "Metodë e kombinuar autentifikimi" është një mënyrë e përbërë nga dy ose më shumë elementë sigurie.

18. "Veprim i privilegjuar" përfshin, por pa u kufizuar në, ndryshimin e konfigurimeve të sistemit, ndryshimin e parametrave të sistemit, aksesin në loget e auditimit dhe sigurisë, aksesin në të dhëna, skedar dhe llogari që përdoren nga përdoruesit e tjerë përfshirë *back-up*-et dhe mediat elektronike.

19. "Konfidencialiteti" është aftësia për të provuar që informacioni nuk është i ekspozuar për entitete të paautorizuara.

20. "Integriteti" është aftësia për të ruajtur saktësinë dhe plotësinë e aseteve.

21. "Disponueshmëria" është aftësia e aseteve për të qenë të arritshme dhe të përdorshme kur nevojiten.

22. "Autenticiteti" është aftësia për të provuar se informacioni është i vërtetë dhe nga burime të sigurta.

23. "Pamohueshmëria" është aftësia për të provuar që një veprim ose ngjarje ka ndodhur, në mënyrë që ngjarja ose veprimi nuk mund të mohohen më vonë.

24. "Material kriptografik" përfshin çelësat në të gjitha format e tyre, dokumentet, pajisjet që përmbajnë informacion kriptografik e që janë të rëndësishëm për kriptimin dhe dekriptimin e informacionit.

25. "Autorizim kripto" është dokumenti që autorizon një individ për të aksesuar ose menaxhuar materialet kriptografike.

26. Mjedis i sigurt global i sistemit (MSG - *global secure environment*) është rrethina e objektit ku është instaluar dhe operon sistemi.

27. Mjedis i sigurt lokal i sistemit (MSL)" është objekti ku është instaluar dhe operon sistemi.

28. "Mjedis i sigurt elektronik i sistemit (MSE)" janë sistemi *software* dhe *hardware*.

29. "Mënyra e dedikuar" është mënyra e operimit në të cilën të gjithë individët me të drejtë aksesi në SKI janë të certifikuar në nivelin më të lartë të klasifikimit që trajtohet në SKI dhe me nevojë të përbashkët për njohje për të gjithë informacionin që trajtohet në SKI.

30. "Mënyra e lartë" është mënyra e operimit në të cilën të gjithë individët me të drejtë aksesi në SKI janë të certifikuar në nivelin më të lartë të klasifikimit që trajtohet në SKI, por jo të gjithë individët kanë të njëjtën nevojë për njohje për informacionin që ruhet, përpunohet ose transmetohet në sistem. Aprovimi për akses në informacionin që trajtohet në sistem jepet në nivel individual sipas funksionit që ka individi.

31. "Mënyra me shumë nivele" është mënyra e operimit në të cilën jo të gjithë individët me të drejtë aksesi në SKI janë të certifikuar në nivelin më të lartë të klasifikimit që trajtohet në SKI dhe jo të gjithë individët me të drejtë aksesi në SKI kanë të njëjtën nevojë për njohje me informacionin që ruhet, përpunohet ose transmetohet në sistem.

32. Ndërlidhje e sistemeve nënkupton lidhjen direkte të dy ose më shumë SKI-ve me qëllim shkëmbimin e të dhënave ose shërbimeve.

Neni 4

Objektivat e sigurisë

1. Objektivat e sigurisë, janë:

a) Konfidencialiteti – të sigurohet konfidencialiteti i informacionit nëpërmjet kontrollit të aksesit në informacionin e klasifikuar, shërbimet dhe burimet e sistemit.

b) Integriteti – të sigurohet integriteti i informacionit të klasifikuar, i shërbimeve dhe burimeve të sistemit.

c) Disponueshmëria - të sigurohet disponueshmëria e informacionit të klasifikuar, i shërbimeve dhe burimeve të sistemit.

d) Autenticiteti - të sigurohet identifikimi dhe autentifikimi i personave, pajisjeve dhe shërbimeve që aksesojnë SKI-të që trajtojnë informacion të klasifikuar.

e) Pamohueshmëri – të sigurohet mos refuzimi i entiteteve që kanë përpunuar informacion.

2. Niveli i aplikimit të këtyre objektivave të sigurisë është specifik për SKI të ndryshme dhe përcaktohet nga misioni i sistemit, kërkesat minimale të sigurisë dhe rezultatet e procesit të menaxhimit të riskut.

Neni 5
Kriteret themelore të sigurisë

1. SKI-të ndjekin këto kritere sigurie:

a) Menaxhimi i riskut të sigurisë: Aplikimi i procesit të menaxhimit të riskut për monitorimin, reduktimin, eliminimin, shmangien ose pranimin e riskut që lidhet me sigurinë e SKI-ve.

b) Funksionalitetet dhe privilegjet minimale: Instalimi dhe përdorimi vetëm i funksioneve, protokolleve dhe shërbimeve që kërkohen për të përmbushur misionin operacional të sistemit. Entitetit që përdor SKI-në i lejohen vetëm privilegjet dhe autorizimet që nevojiten për kryerjen e detyrave.

c) Nyja vetëmbrojtëse. Secili SKI i ndërlidhur të trajtojë SKI-në tjetër si të huaj dhe të implementohen masa për kontrollin e shkëmbimit të informacionit me SKI-në tjetër.

d) Mbrojtja shumënivelëshe. Masat e sigurisë së SKI-ve të implementohen në mënyrë të tillë që të ketë më shumë se një nivel mbrojtjeje.

e) Përditësimi i masave të sigurisë. Rishikim herë pas herë i implementimit dhe efektivitetit të masave të sigurisë së SKI-ve në varësi të ndryshimeve në mjedisin e kërcënimeve dhe dobësive.

f) Akreditimi i SKI-ve. Akreditimi i SKI-ve përshtatshmërisht me nivelin e informacionit që trajtohet në to.

2. DSIK verifikon periodikisht aplikimin e këtyre kritereve dhe implementimin e vazhdueshëm të standardeve të sigurisë.

PJESA I
QEVERISJA E SIGURISË SË INFORMACIONIT

KREU I
AUTORITETET E SIGURISË

Neni 6
Autoritetet e sigurisë së SKI-ve

Për vlerësimin dhe trajtimin e aspekteve të sigurisë së SKI-ve krijohen këto autoritete sigurie.

1. Autoriteti Kombëtar i Akreditimit të Sigurisë (AKAS).
2. Autoriteti Kombëtar i Testimit, Vlerësimit dhe Certifikimit të Sigurisë (AKTVCS).
3. Autoriteti Kombëtar i Sigurisë së Komunikimeve (AKSK).
4. Autoriteti Kombëtar i Shpërndarjes (AKSH).
5. Autoriteti Kombëtar TEMPEST (AKT).

6. Autoriteti Kombëtar i Mbrojtjes Kibernetike (AKMK).
7. Autoriteti i Operimit të Sistemit (AOS).

Neni 7
Autoriteti Kombëtar i Akreditimit të Sigurisë (AKAS)

1. Autoriteti Kombëtar i Akreditimit të Sigurisë (AKAS) është përgjegjës për akreditimin e sigurisë së SKI-ve që trajtojnë informacion të klasifikuar, në një nivel të caktuar klasifikimi në mjedisin e tyre operacional. Autoriteti Kombëtar i Akreditimit të Sigurisë është Drejtoria e Sigurimit të Informacionit të Klasifikuar .
2. AKAS-i ka këto detyra:
a) Shqyrton kërkesat për akreditimin e sistemeve;
b) Bashkëpunon me autoritetet e sigurisë për identifikimin e komponentëve dhe sistemit që duhet të testohet, vlerësohet dhe certifikohet.
c) Përcakton rolet dhe përgjegjësitë e strukturave të sigurisë, kushtet në të cilat do të akreditohet sistemi dhe harton e miraton Planin e Akreditimit të Sigurisë së Sistemit.
d) Koordinon punën për akreditimin e sigurisë së sistemeve me strukturat përkatëse të sigurisë;
e) Verifikon zbatimin e masave të sigurisë për mbrojtjen e informacionit të klasifikuar gjatë përpunimit, ruajtjes ose transmetimit në sistemet e komunikimit dhe të informacionit nga cënimi aksidental ose i qëllimshëm i objektivave të sigurisë:
i) Verifikon zonat e sigurisë ku është instaluar dhe operon sistemi;
ii) Verifikon nëse përdoruesit e sistemit janë të pajisur me certifikata sigurie;
iii) Verifikon nëse aplikohen aspekte të sigurimit industrial;
iv) Verifikon nëse aplikohen marrëveshje sigurie me struktura të tjera brenda apo jashtë vendit;
v) Verifikon dokumentacionin e sigurisë së sistemit;
vi) Verifikon zbatimin e kërkesave të sigurisë së komunikimeve, sigurisë kriptografike dhe sigurisë së emetimeve, nëse aplikohen, në bashkëpunim me autoritetet e sigurisë;
vii) Inspekton MSG/MSL;
viii) Verifikon nëse masat e sigurisë së sistemit janë në përputhje me Planin e Menaxhimit të Riskut.
f) Analizon dhe vlerëson gjendjen e sigurisë së sistemit në varësi të dokumentacionit të sigurisë së sistemit, dokumenteve të lëshuar nga autoritetet e sigurisë dhe rezultateve të inspektimeve.
g) Pranon riskun e mbetur të sistemit dhe harton akt vlerësimin për zbatimin e masave të sigurisë.
h) Lëshon deklaratën e akreditimit, që autorizon sistemin për të trajtuar informacion të klasifikuar. Kjo deklaratë lëshohet bazuar në vlerësimin pozitiv të sigurisë së SKI-s.
i) Menaxhon databazën e sistemeve të klasifikuar kombëtare, të NATO-s, shteteve dhe organizatave të huaja të akredituar nga DSIK.
j) Trajnon personelin/strukturat e SKI mbi aspekte të përmbushjes së detyrimeve për akreditimin e sigurisë.

Neni 8
Autoriteti i Operimit të Sistemit (AOS)

1. Institucionet shtetërore që kanë në zotërim një ose më shumë SKI marrin rolin e Autoritetit të Operimit të Sistemit (AOS).
2. Autoriteti i Operimit të Sistemit (AOS) është përgjegjës për administrimin e përditshëm të operimit të sigurt të sistemit si dhe aspekteve të ndërlidhjes së sistemit me sisteme të tjera.

3. AOS-ja ka këto detyra:

a) Është përgjegjës për operimin e sigurt të sistemeve të klasifikuar që ka në zotërim.

b) Është përgjegjës për të kërkuar akreditimin e sistemeve dhe menaxhuar sistemet e akredituara që ka në zotërim.

c) Cakton Oficerin/Strukturën e Sigurisë së SKI-ve për menaxhimin e aspekteve të sigurisë së sistemeve, përgjegjës për garantimin e përputhshmërisë së masave të sigurisë së SKI-ve me politikat, standardet dhe legjislacionin për informacionin e klasifikuar "Sekret shtetëror".

2. Kjo strukturë:

i. Formulon dhe mirëmban dokumentet e sigurisë së sistemit, në bashkëpunim me personin/strukturën përgjegjëse për implementimin dhe monitorimin e masave të sigurisë teknike të SKI-ve.

ii. Këshillon mbi sigurinë e SKI-së dhe ndërgjegjëson administratorët dhe përdoruesit e sistemit, përfshirë nivelet drejtuese, për aspektet e sigurisë së SKI-së;

iii. Mirëmban listën e personave të autorizuar për përdorimin e SKI-së si dhe nivelin e autorizimit dhe siguron që këta persona janë të certifikuar përshtatshmërisht dhe kanë nevojë për njohje për informacionin që trajtohet në SKI;

iv. Kryen ose koordinon ekzekutimin e vlerësimeve periodike të sigurisë së SKI-së (p.sh. vlerësim risku, testim dhe vlerësim i sigurisë, inspektim i sigurisë, vlerësim i dobësive);

v. Raporton në instancat përkatëse mbi mangësitë dhe dobësitë e konstatuara që lidhen me sigurinë e SKI-së;

vi. Menaxhon dhe investigon incidentet e sigurisë së SKI-së në bashkëpunim me strukturën e sigurisë sipas rastit, dhe raporton në instancat përkatëse.

Neni 9

Autoriteti Kombëtar i Testimit, Vlerësimit dhe Certifikimit të Sigurisë (AKTVCS)

1. Autoriteti Kombëtar i Testimit, Vlerësimit dhe Certifikimit të Sigurisë është Drejtoria e Sigurimit të Informacionit të Klasifikuar (Autoritet i Sigurisë Kombëtare).

2. AKTVCS ka këto detyra:

a) Përcaktimin e komponentëve specifikë të sistemit që duhet të testohen dhe vlerësohen, masave të sigurisë dhe pritshmërive për secilin element;

b) Përzgjedhjen, përgatitjen dhe aprovimin e procedurave dhe metodave të testimit dhe vlerësimit të komponentëve specifikë të sistemit;

c) Përzgjedhjen e mjeteve të testimit të komponentëve specifikë të sistemit;

d) Auditimin e implementimit të kërkesave të sigurisë në sistem dhe vlerësimin e operimit korrekt të masave të sigurisë të implementuara në sistem;

e) Vlerësimin e nivelit të përputhshmërisë së dokumentacionit të sistemit dhe zbatimit në praktikë të masave të deklaruara në dokumentacion për MSE;

f) Kryerjen e aktiviteteve të testimit të kontrolleve specifike teknologjike: hardware, software, të sistemit operativ, aplikacioneve dhe databazave në sistem;

g) Testimin dhe vlerësimin e dobësive të sistemit;

h) Kontribuon në vlerësimin e riskut të sigurisë së sistemit;

i) Dokumentimin e saktë të procedurave dhe rezultateve të testimit dhe gjenerimin e raporteve të vlerësimit të sigurisë;

j) Lëshimin e certifikatës së sigurisë së sistemit bazuar në raportet e vlerësimit të sigurisë, sipas rasteve të parapërcaktuara në Planin e Akreditimit të Sigurisë së Sistemit;

k) Menaxhon databazën e sistemeve të certifikuar nga DSIK.

Neni 10

Autoriteti Kombëtar i Sigurisë së Komunikimeve (AKSK)

1. Autoriteti Kombëtar i Sigurisë së Komunikimeve është Drejtoria e Shifrës.

2. AKSK-i ka këto detyra kryesore:

a) Përcakton kërkesat e sigurisë specifike për sistemet, produktet dhe mekanizmat kriptografikë dhe kontrollon zbatimin e tyre nga institucionet shtetërore;

b) Përcakton procedurat për përzgjedhjen, operimin dhe mirëmbajtjen e sistemeve, produkteve dhe mekanizmave kriptografikë dhe kontrollon zbatimin e tyre nga institucionet shtetërore;

c) Administron infrastrukturën e materialit kriptografik të pajisjeve/sistemeve të përzgjedhur.

d) Vlerëson sistemet, produktet dhe mekanizmat kriptografikë dhe harton Akt vlerësimin përkatës dhe ia përcjell AKAS në funksion të procesit të akreditimit të sigurisë;

e) Inspekton strukturat kriptografike në institucionet shtetërore për masat për zbatimin e mbrojtjes kriptografike të informacionit të klasifikuar, instalimin, ruajtjen dhe mirëmbajtjen e pajisjeve, sistemeve dhe incidentet kriptografike;

f) Menaxhon databazën e sistemeve, produkteve dhe mekanizmave kriptografikë të vlerësuar dhe që përdoren nga institucionet shtetërore.

Neni 11

Autoriteti Kombëtar i Shpërndarjes (AKSH)

1. Autoriteti Kombëtar i Shpërndarjes është Drejtoria e Shifrës.

2. AKSH ka këto detyra:

a) Administron materialet kriptografike që përdoren për mbrojtjen e informacionit të klasifikuar.

b) Mban databazën e pajisjeve dhe programeve kriptografike, materialit çelës, dokumenteve e procedurave përkatëse për menaxhimin e tyre;

c) Shpërndan materialin kriptografik në institucionet shtetërore;

d) Administron sistemet e shkëmbimit elektronik të çelësave kriptografikë dhe të llogarisë së materialit kriptografik kombëtar, të NATO-s, BE-së, shteteve dhe organizatave të tjera ndërkombëtare.

e) Zbaton rregullat e sigurimit fizik dhe elektronik sipas akteve nënligjore në fuqi për ruajtjen e materialit kriptografik;

f) Siguron që materiali kriptografik të jetë në çdo kohë në kushte pune;

g) Shkatërron materialin kriptografik, sipas rregullores kur është e nevojshme;

h) Harton procedurat që duhen ndjekur për raportimin e incidenteve;

i) Harton procedurat që duhen ndjekur ne rastet e emergjencës;

j) Siguron që i gjithë personeli që ka akses në materialin kriptografik është i autorizuar, i certifikuar dhe i trajnuar sipas akteve nënligjore në fuqi.

Neni 12

Autoriteti Kombëtar TEMPEST (AKT)

1. Autoriteti Kombëtar TEMPEST është Drejtoria e Shifrës.

2. AKT ka këto detyra:

a) Harton politika, standarde e procedura për mbrojtjen nga emetimet elektromagnetike kompromentuese;

b) Përzgjedh, siguron dhe administron pajisjet elektronike për realizimin e matjeve TEMPEST të ambienteve dhe pajisjeve;

c) Kryen periodikisht matjet TEMPEST, dhe përgatit raportin me rezultatet e matjeve për DSIK-në dhe institucionet përkatëse;

d) Kontrollon dhe rekomandon masat që duhen zbatuar për të mënjanuar riskun nga emetimet elektromagnetike kompromentuese;

e) Mban databazën me historikun e rezultateve të matjeve TEMPEST.

Neni 13

Autoriteti Kombëtar i Mbrojtjes Kibernetike (AKMK) për SKI –të

.

1. Autoriteti Kombëtar i Mbrojtjes Kibernetike (AKMK) është Drejtoria e Sigurimit të Informacionit të Klasifikuar (Autoritet i Sigurisë Kombëtare).

2. AKMK ka këto detyra:

a) Harton dhe zhvillon konceptet, stategjinë, politikat etj., për mbrojtjen kibernetike të sistemeve të klasifikuar;

b) Zhvillon procedurat dhe standardet teknike në përputhje me përcaktimet e NATO-s dhe ato Evropiane;

c) Organizon dhe realizon ndërgjegjësimin, edukimin dhe trajnimin e personelit për mbrojtjen kibernetike;

d) Siguron ndërveprimin me strukturat përkatëse shtetërore, të NATO-s, BE-së dhe organizatave të tjera ndërkombëtare për të zhvilluar konceptin e mbrojtjes kibernetike si dhe të masave reaguese;

e) Shërben si pikë kontakti me struktura të tjera homologe jashtë vendit;

f) Evidenton, vlerëson dhe paralajmëron për rreziqet dhe kërcënimet kibernetike;

g) Teston dhe vlerëson masat e mbrojtjes kibernetike;

h) Rekomandon dhe këshillon për implementimin e masave të sigurisë;

i) Përcakton mjetet e nevojshme teknike për evidentimin dhe reagimin ndaj incidenteve;

j) Siguron monitorimin e vazhdueshëm të sistemeve të klasifikuara, nëpërmjet nënstrukturave të ngritura në ministri e institucione shtetërore;

k) Mbledh dhe regjistron informacion në lidhje me cenimin e sigurisë së sistemeve të komunikimit dhe të informacionit dhe administron listën e incidenteve të ndodhura më parë në këto sisteme;

l) Azhurnon listën e kërcënimeve të reja që mund të ndodhin në SKI-të;

m) Shpërndan informacionin me strukturat e tjera përgjegjëse që përballen me kërcënimet e reja;

n) Punon për reduktimin e dobësive të SKI-ve;

o) Punon për të ulur mundësinë e krizave në SKI;

p) Punon për njohjen e shtrirjes së kërcënimeve në SKI-të;

q) Përcakton një shkallë matëse për sulmet duke filluar nga sulmet më të thjeshta tek ato më të komplikuara dhe me shkallë më të gjerë;

r) Përcakton dhe klasifikon riskun dhe kërcënimet në fushën e mbrojtjes kibernetike dhe siguron që masat e marra u paraprijnë incidenteve që mund të ndodhin.

3. AKMK në rast krize në SKI:

a) Përgjigjet në mënyrë të menjëhershme duke marrë masa reaguese ndaj sulmeve kibernetike për minimizimin / eliminimin e riskut dhe tejkalimin e krizës;

b) Kufizon shtrirjen më të gjerë të krizës;

c) Mbledh dhe analizon rezultatet.

KREU II
MENAXHIMI I RISKUT TË SIGURISË SË INFORMACIONIT

Neni 14

Identifikimi dhe vlerësimi i riskut të sigurisë

Institucionet shtetërore të identifikojnë dhe vlerësojnë riskun e sigurisë në informacionin dhe SKI-të që kanë në zotërim.

Neni 15
Procesi i Menaxhimit të Riskut

1. Institucionet shtetërore implementojnë një metodë të menaxhimit të riskut për të mbuluar të gjitha aspektet e sigurisë së informacionit, e cila miratohet nga titullari i institucionit.
2. Institucionet shtetërore kryejnë proceset e menaxhimit të riskut të sigurisë për monitorimin, reduktimin, eliminimin, shmangien ose pranimin e rreziqeve që lidhen me SKI-të.
3. Procesi i menaxhimit të riskut të sigurisë kryhet nga përfaqësues të disiplinave të ndryshme për mbrojtjen e informacionit të klasifikuar.
4. Procesi i menaxhimit të riskut përfshin:
a) Identifikimin dhe vlerësimin e aseteve;
b) Identifikimin e agjentëve kërcënues (person, proces kompjuterik, pajisje etj);
c) Identifikimin e kërcënimeve që vijnë si pasojë e veprimit të agjentëve;
d) Identifikimin e dobësive që mund të shfrytëzohen nga agjentët kërcënues;
e) Identifikimin e riskut;
f) Vlerësimin e masave ekzistuese të sigurisë;
g) Vlerësimin e riskut ose përcaktimin e nivelit të riskut;
h) Identifikimin e masave përkatëse për monitorimin, reduktimin, eliminimin, shmangien ose pranimin e riskut;
i) Përcaktimin e riskut të mbetur.

Neni 16
Plani i Menaxhimit të Riskut

1. Institucionet shtetërore të dokumentojnë riskun e sigurisë si dhe procesin e menaxhimit të tij në Planin e Menaxhimit të Riskut.
2. Plani i Menaxhimit të Riskut përfshin:
a) Rolet dhe përgjegjësitë e anëtarëve të grupit për menaxhimin e riskut;
b) Objektivat e grupit për menaxhimin e riskut;
c) Proceset formale të identifikimit të riskut;
d) Lidhjen e riskut me masat ekzistuese.

Neni 17
Risku i mbetur

1. Risku i sigurisë që konsiderohet si i pranueshëm miratohet formalisht nga DSIK gjatë procesit të akreditimit të sigurisë së SKI-ve dhe mbahet nën monitorim të vazhdueshëm nga Autoriteti i Operimit të Sistemit.
2. Risku i sigurisë që konsiderohet si i papranueshëm duhet të trajtohet nëpërmjet aplikimit të masave shtesë ose masave alternative të sigurisë.

KREU III
DOKUMENTACIONI I SIGURISË SË SISTEMIT

Neni 18
Dokumentacioni i sigurisë së sistemit

1. Dokumentacioni i sigurisë së sistemit është tërësia e dokumentave që kërkohen për akreditimin e sigurisë së SKI-së dhe shërben si standard për vlerësimin e tij.
2. Dokumentacioni i sigurisë së sistemit:

a) Hartohet nga personeli/struktura e sigurisë së SKI-së;

b) Përmbajtja e dokumenteve të jetë në përputhje me legjislacionin për sigurinë e informacionit. dhe të përcaktojë qëllimin, kërkesat e sigurisë, masat e sigurisë së SKI-së që do të akreditohet si dhe përgjegjësitë dhe autoritetet e institucioneve të përfshira në procesin e akreditimit të sigurisë;

c) Miratohet nga titullari i institucionit;

d) I vihet në dispozicion personelit që ka akses në sistem në përputhje me nevojën për njohje;

e) Përditësohet rregullisht.

3. Dokumentacioni i sigurisë së sistemit përbëhet nga:

a) Udhëzim për sigurinë e SKI-ve;

b) Koncepti i Operimit (KO);

c) Deklarata e Përbashkët e Kërkesave të Sigurisë (DPKS);

d) Deklarata e Kërkesave të Sigurisë së Ndërlidhjes së Sistemit (DKSNS);

e) Deklarata e Kërkesave të Sigurisë Specifike të Sistemit (DKSSS);

f) Procedurat e Operimit të Sigurt (POS);

g) Plani i Menaxhimit të Riskut (PMR);

h) Procedurat e Testimit dhe Vlerësimit të Sigurisë (PVTS);

i) Plani i përgjigjes ndaj incidenteve;

j) Procedurat në rastet e emergjencave;

k) Urdhri për ndarjen e Zonave të Sigurisë.

4. Gjatë procesit të akreditimit të sigurisë së sistemit gjenerohen dokumente shtesë, të cilat i bashkëlidhen dokumentacionit të sigurisë së sistemit, ku përfshihen:

a) Plani i Akreditimit të Sigurisë së Sistemit (PASS);

b) Raporti i rezultateve të matjeve TEMPEST të Mjediseve;

c) Plani i menaxhimit të materialeve kriptografikë;

d) Plani i Testimit dhe Vlerësimit të Sigurisë së Komponentëve të Sistemit (PVTSKS);

e) Raportet e testimit dhe vlerësimit të sigurisë;

f) Raportet e inspektimit;

g) Certifikata TEMPEST e pajisjeve (nëse aplikohet);

h) Deklarata e Akreditimit të Sigurisë.

Neni 19

Rishikimi i dokumentacionit

1. Dokumentacioni i sigurisë së sistemit rishikohet në këto raste:

a) Periodikisht minimumi një herë në vit.

b)Në përgjigje të ndryshimeve në sistem, mjedis ose operimin e sistemit.

2. Dokumentacioni i sigurisë së sistemit duhet të ketë të regjistruar datën e rishikimit të fundit.

Neni 20

Kërkesa të tjera shtesë për dokumentacionin

1. AKAS-i ka të drejtë të kërkojë dokumente shtesë, nëse e gjykon të nevojshme për sistemet e integruara në programe ndërkombëtare.

2. Për sistemet e shteteve ose organizatave ndërkombëtare dokumentet plotësohen në 2 kopje, një në gjuhën angleze dhe një në gjuhën shqipe.

KREU IV
AKREDITIMI I SIGURISË SË SKI

Neni 21
Të përgjithshme

1. Sistemet që trajtojnë informacion të klasifikuar duhet të akreditohen në përputhje me kërkesat e përcaktuara në këtë rregullore.

2. Institucionet shtetërore janë përgjegjëse për inicimin e kërkesave për akreditimin e sigurisë së SKI-ve që operojnë ose duan të operojnë.

3. DSIK është përgjegjës për ndjekjen e procesit të akreditimit të sigurisë së SKI-ve.

4. Procesi i akreditimit të sigurisë përcakton nivelin e përshtatshëm të mbrojtjes së sistemit si dhe identifikon dhe pranon riskun e mbetur, që duhet të monitorohet përgjatë jetëgjatësisë së sistemit.

5. DSIK-ja mban, administron dhe përditëson bazën qendrore të të dhënave ku pasqyrohen të gjitha kërkesat për akreditim si dhe statusi i akreditimit të SKI-ve kombëtare dhe shteteve apo organizatave ndërkombëtare që operojnë në institucionet shtetërore.

Neni 22
Mjediset e sigurisë së sistemeve

1. Ndarja e mjediseve të sigurisë së sistemeve bëhet me qëllim përcaktimin e përgjegjësive për sigurinë e SKI-ve.

2. Mjediset e sigurisë së sistemeve janë:

a) Mjedisi i Sigurisë Globale (MSG) përfaqëson zonën e sigurisë ku ndodhet sistemi, por që është jashtë kontrollit të AOS. MGS përfshin aspektet e sigurisë së ndërtesës ose të site-t, vendndodhjen gjeografrike, sigurinë e ndërlidhjes së sistemeve dhe mjedisin e përgjithshëm të kërcënimeve.

b) Mjedisi i Sigurisë Lokale (MSL) është zona e sigurisë nën ndikimin e AOS. MLS përfshin masat e sigurimit fizik, sigurisë së personelit, sigurisë së informacionit dhe sigurisë procedurale.

c) Mjedisi i Sigurisë Elektronike (MSE) është zona e sigurisë që përfshin mekanizmat e sigurisë elektronike të SKI-ve të implementuar brenda arkitekturës së sigurisë së sistemit dhe që ofrojnë funksionet e nevojshme të sigurisë. MSE përfshin:

i) ndërfaqet individ-makinë;

ii) ndërfaqet e brendshme (ndërfaqet ndërmjet pjesëve të sistemit që përfaqësojnë klasa të ndryshme të sigurisë p.sh. particionet e sigurisë në sistem);

iii) ndërfaqet e jashtme (ndërfaqet e sistemeve me DSS të ndryshme ose të aprovuar nga AKAS të ndryshme, *firewalle, gateway* etj.).

Neni 23
Mënyra e sigurisë së operimit të sistemit

1. SKI-të që trajtojnë informacion të klasifikuar në nivel "Konfidencial" e lart të operojnë në një nga mënyrat e mëposhtme të sigurisë:

a) Mënyrë e dedikuar.

b) Mënyrë e lartë.

c) Mënyrë me shumë nivele.

2. SKI-të që trajtojnë informacion të klasifikuar në nivel "i Kufizuar" të operojnë në një nga mënyrat e mëposhtme të sigurisë:

a) Mënyrë e dedikuar.

b) Mënyrë e lartë.

Neni 24
Bazat e akreditimit të sigurisë

Bazë për akreditimin e sigurisë së SKI-së konsiderohet si më poshtë:

1. Vlerësimi i arkitekturës së sigurisë së sistemit.

2. Vlerësimi i dokumentacionit të sigurisë së sistemit.

3. Verifikimi i implementimit dhe efektivitetit të masave të sigurisë së SKI-së, nëpërmjet testimeve të komponentëve të caktuar të sistemit bazuar në planin e T&VS si dhe nëpërmjet inspektimit të ambienteve ku shtrihet sistemi dhe intervistimit të personave që punojnë në sistem ose menaxhojnë aspektet e sigurisë së informacionit.

4. Analiza e riskut të mbetur dhe proceseve për menaxhimin e vazhdueshëm të riskut të sigurisë.

5. Monitorimi i vazhdueshëm i statusit të sigurisë së SKI-së.

Neni 25
Procesi i akreditimit të sigurisë

1. Procesi i akreditimit të sigurisë është tërësia e hapave që duhet të ndërmerren për të përcaktuar nëse masat e sigurisë së sistemit janë implementuar sipas kërkesave të kësaj rregulloreje. Procesi i akreditimit të sigurisë është mekanizmi që garanton sigurinë e SKI-ve.

2. Procesi i akreditimit të sigurisë ndryshon në varësi të arkitekturës së SKI-së, në përputhje me këtë rregullore.

3. Procesi i akreditimit të sigurisë përfshin dy nivele:

a) Certifikimi.

b) Akreditimi.

Neni 26
Fazat e procesit të akreditimit të sigurisë

Procesi i akreditimit kalon në fazat si më poshtë:

1. Fillimi i procesit;

2. Verifikimi i sistemit;

3. Miratimi;

4. Aktivitet pas akreditimit.

Neni 27
Fillimi i procesit

1. Fillimi i procesit të akreditimit ka si objektiv njohjen me misionin e sistemit, përshkrimin e aspekteve funksionale dhe arkitekturën e sigurisë së sistemit, caktimin e roleve dhe përgjegjësive, me qëllim përcaktimin e kërkesave për akreditimin e sistemit.

2. Kjo fazë përfshin këto aktivitete:

a) inicimi i kërkesës:

i. kërkesa për akreditimin e sistemit drejtuar DSIK-së, duhet të përfshijë përshkrimin e sistemit sipas konceptit të operimit;

ii. pas marrjes së kërkesës, DSIK-ja e konsideron procesin e akreditimit të hapur dhe kërkon shpjegime të nevojshme ose korrigjime, nëse nevojitet;

iii. në rastet e kërkesës për riakreditim dërgohet versioni i fundit i Konceptit të Operimit;

b) negocimi, fazë në të cilën hartohet PASS:

i) AOS-i raporton tek AKAS-i datën në të cilën sistemi dhe mjedisi i sigurisë së tij (mjedisi i sigurisë lokale, globale dhe elektronike) janë gati për verifikim, në mënyrë që AKAS-i të skedulojë planin e akreditimit të sigurisë;

ii) AOS-i duhet të raportojë tek AKAS çdo lloj kushti shtesë (operacional, komercial ose strategjik), nëse ka, për t'u marrë në konsideratë nga AKAS-i për t'i dhënë prioritet akreditimit të këtij sistemi në fazat pasardhëse të procesit;

c) implementimi dhe dokumentimi i masave të sigurisë:

i. AOS-i, pas aprovimit të konceptimit të operimit, marrin masat për përgatitjen e dokumentacionit të sigurisë së sistemit, si dhe identifikimin dhe përmbushjen e aktiviteteve për akreditimin e sistemit;

ii. dokumentacioni i sigurisë së sistemit, së bashku me dokumente të tjera shtesë për aspekte të sigurisë së personelit, sigurimit industrial etj., dërgohet tek AKAS-i për aprovim;

iii. AOS-i, është përgjegjës për implementimin e sistemit në përputhje me dokumentacionin e dorëzuar në DSIK dhe masat e sigurisë të përshkruara në të.

Neni 28
Verifikimi i sistemit

1. Verifikimi ka si objektivë rishikimin e dokumentacionit të sigurisë së sistemit dhe verifikimin e masave të sigurisë së sistemit me qëllim konfirmimin e sigurisë së sistemit dhe identifikimin e kërkesave të sigurisë që nuk janë përmbushur dhe dobësitë e sistemit.

2. Kjo fazë përfshin këto aktivitete :

a) testim dhe vlerësim i sigurisë;

b) testim i penetrimit në sistem;

c) analizë e menaxhimit të sistemit;

d) matjet TEMPEST të zonave të sigurisë;

e) rishikim i menaxhimit të riskut.

3. Autoritetet e sigurisë kryejnë verifikimin e masave të sigurisë në përputhje me PASS dhe dokumentojnë rezultatet dhe riskun e mbetur në raportet përkatëse të testimit dhe vlerësimit.

4. AOS, përditësojnë sistemin dhe dokumentacionin me rekomandimet e rezultateve të verifikimit për ta bërë sistemin gati për akreditim.

5. Verifikimi i masave të sigurisë së sistemit kryhet me një nga këto metoda:

a) testim;

b) ekzaminim;

c) intervistim.

Neni 29
Miratimi

1. Miratimi ka si objektiv autorizimin e sistemit për të operuar brenda kushteve të sigurisë.

2. Kjo fazë përfshin këto aktivitete:

a) certifikim: Autoritetet e sigurisë që kanë kryer verifikimin e masave të sigurisë lëshojnë certifikatën e sigurisë përkatëse për komponentët e sistemit që kanë verifikuar.

b) akreditim: AKAS-i verifikon dokumentacionin e sigurisë së sistemit, përfshirë raportet e vlerësimit dhe certifikatat e sigurisë, inspekton zbatimin e masave të sigurisë, vlerëson riskun e mbetur.

Neni 30
Akreditimi i Sigurisë

1. AKAS-i vendos, për:

a) Lëshimin e Deklaratës së Akreditimit të Sigurisë për një periudhë të caktuar kohore për mjedisin e planifikuar operacional, në të cilin përmbushen të gjithë kërkesat e sigurisë; Deklarata e Akreditimit të Sigurisë përcakton kushtet nën të cilat është i vlefshëm akreditimi i sigurisë. Periudha e vlefshmërisë së akreditimit ndryshon në varësi të nivelit të klasifikimit si më poshtë:

b) Tepër Sekret ose ekuivalent – 3 vjet;

c) Sekret ose ekuivalent – 3–4 vjet;

d) Konfidencial ose ekuivalent – 4–5 vjet;

e) I kufizuar ose ekuivalent – 5–7 vjet;

f) Lëshimin e Deklaratës së Përkohshme të Akreditimit të Sigurisë për një periudhë të caktuar kohore për mjedisin e planifikuar operacional, në të cilin nuk janë përmbushur të gjithë kërkesat e sigurisë. Deklarata e Përkohshme e Akreditimit të Sigurisë përcakton periudhën e vlefshmërisë si dhe kushtet dhe aktivitetet që duhen kryer për të kaluar në Deklaratë të Akreditimit të Sigurisë.

g) Lëshimin Autorizimit për Operim të Kufizuar autorizim i kështillueshëm nëse procesi i akreditimit nuk ka mbaruar. Ky lloj autorizimi lëshohet vetëm në rrethana të jashtëzakonshme, kur kërkesat operacionale tejkalojnë kërkesat e sigurisë (deri në 6 muaj, pa të drejtë shtyrje). Për këtë lloj autorizimi duhet më parë të miratohet koncepti i operimit.

h) Refuzimin e akreditimit të sigurisë; këtu përfshihet identifikimi i mangësive specifike dhe masave korrigjuese. AKAS-i i kërkon AOS-së hartimin e planit të veprimit për marrjen e masave korrigjuese.

i) Anulimin e akreditimit ekzistues të sigurisë; këtu përfshihet identifikimi i mangësive specifike dhe masave korrigjuese. AKAS-i i kërkon AOS-së hartimin e planit të veprimit për marrjen e masave korrigjuese.

2. Akreditimi i sistemeve që trajtojnë informacion të klasifikuar të NATO-s, BE-së apo shteteve e organizatave të tjera ndërkombëtare bëhet në përputhje me marrëveshjet e sigurisë për mbrojtjen e ndërsjellë të informacionit të klasifikuar si dhe duke aplikuar këtë rregullore në të gjithë aspektet e mundshme.

Neni 31

Aktivitetet pas akreditimit

1. Aktivitetet pas akreditimit fillojnë pasi sistemi është akreditуar për operim dhe ka si objektiv garantimin e menaxhimit, operimit dhe mirëmbajtës të sigurt të sistemi, si dhe mbajtjen në nivel të pranueshëm të riskut të mbetur.

2. Kjo fazë përfshin këto aktivitete:

a) Përdorimi i sistemit:

i. Pas lëshimit të Deklaratës së Akreditimit të Sigurisë (DAS), AOS është përgjegjës për menaxhimin e sigurisë së sistemit dhe ruajtjen e kushteve të sigurisë nën të cilat u bë i mundur lëshimi i DAS.

ii. AKAS mbikëqyr sigurinë e SKI-ve nën përgjegjësinë e saj nëpërmjet verifikimeve periodike të sigurisë për të garantuar që sistemet e akredituara trajtojnë informacion të klasifikuar në të njëjtat kushte sigurie në të cilat u dha akreditimi.

b) Riakreditim, i cili kryhet në këto raste:

i. Pas përfundimit të periudhës së vlefshmërisë së Deklaratës së Akreditimit të Sigurisë, sistemi nuk është i autorizuar të trajtojë informacion të klasifikuar.

ii. Nëse ndodhin ndryshime në sistem që ndikojnë në kushtet e sigurisë të tilla si:

- Ndryshimet në nivelin e informacionit të klasifikuar që trajtohet në SKI.
- Ndryshimet në kërkesat e sigurisë që vijnë si pasojë e ndryshimeve të legjislacionit për sigurinë e informacionit të klasifikuar.
- Ndryshimet në arkitekturën e sistemit.
- Ndryshimet në konfigurimet e sigurisë së SKI-së.
- Ndryshimet në kërkesat operacionale.

- Identifikimin e kërcënimeve ose dobësive të reja në sisteme.
- Identifikimin e mosfunksionimit të masave të sigurisë.
- Përhapjen e një incidenti të rëndë të sigurisë kompjuterike ose të sigurisë në përgjithësi dhe që ndikon në akreditimin e sigurisë së sistemit.
- Ndryshime të rëndësishme në strukturën fizike të ndërtesës ose të POS-eve.

iii. AOS-i është përgjegjës për njoftimin e AKAS-së për ndryshimet në sistem që në fazën e planifikimit të tyre.

iv. AOS-i është përgjegjëse për inicimin e procedurës së riakreditimit të sistemit 4 muaj para afatit të përfundimit të vlefshmërisë së akreditimit .

c) Nxjerrja jashtë përdorimit e sistemit:

i. AOS-i është përgjegjës për marrjen e masave të përshtatshme për arkivimin ose deklasifikimin dhe/ose shkatërrimin e SKI dhe informacionit që ruhet në të si dhe raportimin tek AKAS-i që në fazën e planifikimit të nxjerrjes jashtë përdorimit.

ii. Procedurat që do të ndiqen përcaktohen në përputhje me legjislacionin në fuqi dhe dokumentet e sigurisë së sistemit.

PJESA II
KËRKESAT E SIGURISË SË SISTEMEVE

KREU I
SIGURIA FIZIKE E SISTEMEVE

Neni 32
Mjediset dhe infrastruktura e rrjetit

1. AOS-i të aplikojnë masat e sigurisë fizike të mjediseve dhe infrastrukturës së rrjetit për mbrojtjen e sistemeve.
2. Sistemet të instalohen dhe operojnë në zona sigurie të klasit I ose II.
3. Në rastet e shkëmbimit të informacionit të klasifikuar në formë elektronike jashtë zonave të sigurisë të aplikohet mbrojtja kriptografike e informacionit.

Neni 33
Sigurimi fizik i serverëve dhe pajisjeve të komunikimit

1. Serverët dhe pajisjet e komunikimit të vendosen në ambiente të veçanta të ndara nga zyrat e përdoruesve.
2. Sallat e serverëve dhe/ose pajisjeve të komunikimit të vendosen në zona sigurie të klasit I.
3. Sallat e serverëve dhe/ose pajisjeve të komunikimit si dhe *rack*-et të sigurohen nga aksesi i paautorizuar ose dëmtimet fizike.
4. Çelësat ose mekanizmat ekuivalentë të aksesit të dhomave të serverëve dhe/ose pajisjeve të komunikimit si dhe *rack*-eve të kontrollohen përshtatshmërisht.
5. Në ambientet ku administrohen materiale ose sisteme të një rëndësie të veçantë (p.sh. materiale kriptografike) të vendosen masa shtesë sigurie si, përforcimi i integritetit të sigurisë nëpërmjet dy personave, ku të gjitha veprimet dëshmohen nga minimalisht një person tjetër i kualifikuar. Në këto zona duhet të sigurohen të gjitha pikat e hyrjeve dhe daljeve.

Neni 34
Sigurimi fizik i pajisjeve dhe mediave kompjuterike

1. Pajisjet dhe mediat elektronike që ruajnë informacion të klasifikuar të regjistrohen në regjistra të veçantë me numër unik identifikimi dhe të ruhen në përputhje me kërkesat e sigurisë, si gjatë orarit zyrtar të punës ashtu edhe jashtë tij. Të kryhen inventarë vjetorë për gjendjen e tyre.

2. Pajisjet dhe mediat elektronike që ruajnë informacion të klasifikuar të administrohen brenda zonave të sigurisë.

3. Në rastet kur nuk është e mundur të aplikohen masat e përshtatshme të sigurimit fizik të pajisjeve dhe mediave kompjuterike, të bëhet fshirja e memories RAM si dhe të përdoret një nga metodat e mëposhtme:

a) përdorimi i hard diskut të jashtëm, i cili të ruhet në kasafortë jashtë orarit zyrtar të punës;

b) konfigurimi i sistemit për të penguar ruajtjen e të dhënave lokalisht;

c) përdorimi i programeve kriptografike për kriptimin e pajisjeve dhe mediave kompjuterike.

KREU II
SIGURIA E PERSONELIT TË SISTEMEVE

Neni 35
Edukimi për sigurinë e informacionit

1. AOS-i ngarkohen me hartimin dhe aplikimin e programeve të edukimit të personelit për sigurinë e informacionit.

2. Qëllimi i këtyre programeve është njohja e personelit me rolet dhe përgjegjësitë, pasojat në rast moszbatimi të rregullave të sigurisë, si dhe risqet e mundshme të sigurisë e masat përkatëse.

Neni 36
Autorizimi, certifikimi dhe brifimi i personelit

1. Aksesi në sistem lejohet vetëm për personat e autorizuar, të certifikuar dhe të brifuar përshtatshmërish për aksesin në sistem.

2. AOS-i kanë detyrë:

a) të kufizojnë aksesin në sistem sipas nevojës për njohje;

b) të lejojnë aksesin në sistem vetëm pas autorizimit të kërkesës për akses dhe njohjen me procedurat e operimit të sigurt të sistemit;

c) t'u japin përdoruesve të drejtat minimale që u nevojiten për kryerjen e detyrave të tyre;

d) të rishikojnë autorizimet dhe të drejtat e aksesit të paktën një herë në vit si dhe kur personeli ndryshon detyrën;

e) gjatë rishikimit të autorizimeve për akses, të konfirmojnë vlefshmërinë e nevojës për aksesimin e sistemit, në të kundërt të heqin të drejtën e aksesit.

3. AOS-i mbajnë rekordet e sakta, për:

a) të gjithë personelin e autorizuar për të aksesuar sistemin;

b) personin/personat që dhanë autorizimin për të aksesuar sistemin;

c) datën e dhënies së autorizimit;

d) datat e rishikimit të autorizimit;

e) datën e heqjes së autorizimit.

4. AOS-i të mbajnë rekordet gjatë gjithë jetëgjatësisë së sistemit në të cilin është lejuar aksesi.

KREU III
SIGURIMI INDUSTRIAL

Neni 37
Siguria industriale

Në rastet e prokurimit të mallrave, punëve dhe shërbimeve për sisteme ku trajtohet informacion i klasifikuar "Sekret shtetëror", operatorët ekonomikë që do të ofrojnë produkte ose shërbime të jenë të certifikuar përshtatshmërish.

Neni 38
Kontratat e klasifikuara

Mallrat, punët dhe shërbimet të cilat do të prokurohen, të jenë si rezultat i kontratave të klasifikuar.

KREU III
SIGURIA E KOMUNIKIMEVE

Neni 39
Infrastruktura e komunikimeve

(Menaxhimi i kabllove)

1. AOS-i të grupojnë kabllot në kanalina si më poshtë:

a) grupi 1 – Kabllot e sistemeve të paklasifikuar;

b) grupi 2 – Kabllot e sistemeve "i Kufizuar", "Konfidencial" dhe "Sekret";

c) grupi 3 – Kabllot e sistemeve "Tepër Sekret".

2. Fibrat optike, pavarësisht grupit ku bëjnë pjesë, mund të grupohen në të njëjtën kanalinë.

3. Kabllot e informacionit të klasifikuar të përfundojnë në kabinete të veçanta.

4. Në rast të niveleve të ndryshme të klasifikimit, kabinetet të ndahen me pllaka ndarëse për secilin nivel klasifikimi.

5. Kabinetet e sistemeve të klasifikuara të jenë në largësi nga kabinetet e sistemeve të paklasifikuar minimalisht 50 cm.

6. Rrjetet e kabllimit të përfundojnë sa më afër kabineteve.

7. Kabllot të etiketohen me numrin unik të identifikimit dhe të shenjëzohen, në pikat e inspektimit, me shenja dalluese sipas skemës së mëposhtme:

a) shirit portokalli – "Tepër Sekret";

b) shirit i kuq – "Sekret";

c) shirit blu – "Konfidencial";

d) shirit i bardhë – "i Kufizuar".

8. Prizat e rrjetit të etiketohen me nivelin e klasifikimit, numrin e kabllos dhe numrin e prizës së rrjetit.

9. Kabllot dhe prizat e rrjetit të dokumentohen në regjistrin e kabllove dhe prizave të rrjetit me numrin përkatës dhe nivelin e klasifikimit. Për secilin kabull të dokumentohet burimi dhe destinacioni.

10. Procedura e etiketimit dhe regjistrimit të kabllove dhe prizave të rrjetit të dokumentohet në POS.

11. Të ndahen fizikisht *patch* panelet e sistemeve të klasifikuar nga ato të paklasifikuar, duke i instaluar ato në kabinete të veçantë.

Neni 40
Siguria e emetimeve

Sistemet që përdoren për trajtimin e informacionit të klasifikuar "Konfidencial" e lart, të mbrohen nga emetimet elektromagnetike kompromentuese, studimi dhe kontrolli i të cilave

referohet si "TEMPEST", sipas rregullave dhe procedurave të specifikuara me rregullore të veçantë.

Neni 41
Sistemet dhe pajisjet e komunikimit

(Pajisjet RF, *infrared* dhe *bluetooth*)

1. Në zonat e sigurisë ndalohet përdorimi i pajisjeve të tilla si:
a) akses point;
b) tastiera *infrared*, *bluetooth* ose *wireless*;
c) pajisje RF.
2. Përjashtim bëhet vetëm në rastet kur merret autorizimi nga AKAS-i.
3. AOS implementojnë masa sigurie për identifikimin e pajisjeve të paautorizuara RF, aktive në zonat e sigurisë.

Neni 42
Sistemet dhe pajisjet e komunikimit
(Pajisjet faks dhe pajisjet faks multifunksionale)

1. AOS-i që përdorin pajisje faks dhe pajisje faks multifunksionale të hartojnë procedurat për përdorimin e sigurt të tyre.
2. AOS-i të përdorin pajisje faks për shkëmbimin e informacionit të klasifikuar të ndryshme nga pajisjet faks të paklasifikuara.
3. AOS-i të sigurojnë që mesazhet faks të jenë të kriptuara në përputhje me nivelin e informacionit që transmetohet.
4. Pajisjet faks multifunksionale, të lidhura me rrjete kompjuterike të klasifikuar, ndalohet të lidhen drejtpërdrejt me rrjete të telefonisë digjitale të paakredituar përshtatshmërish.
5. Pajisjet faks multifunksionale, të lidhura me rrjete kompjuterike të klasifikuar, ndalohet të përdoren për skanimin ose fotokopjimin e dokumenteve në nivel më të lartë klasifikimi.

Neni 43
Telefonat dhe sistemet telefonike

1. AOS-i të hartojnë procedurat për përdorimin e sigurt të telefonave dhe sistemeve telefonike.
2. AOS-i të sigurojnë, që:
a) sistemet telefonike të klasifikuara të akreditohen përshtatshmërish;
b) trafiku i të dhënave të klasifikuara të kriptohet përshtatshmërish.
3. Nuk lejohet përdorimi i telefonave (receptorëve telefonik) pa kordë për informacionin e klasifikuar, pavarësisht nëse lidhet me pajisje të sigurta telefonike.

KREU IV
SIGURIA E TEKNOLOGJISË SË INFORMACIONIT

Neni 44
Siguria e pajisjeve TIK

1. AOS-i të përzgjedhin produkte të vlerësuara sipas një standardi të mirënjohur ndërkombëtar për funksionin e sigurisë që duan të implementojnë.

2. AOS-i të përdorin produkte të vlerësuara sipas një listë të njohur sipas standardeve kombëtare, të NATO-s, BE-së, përveç nëse është vlerësuar, pranuar dhe dokumentuar risku i sigurisë që lidhet me përdorimin e tyre.

3. AOS-i të kontrollojnë dokumentacionin e vlerësimit të produktit, nëse disponohet, të përcaktojnë kërkesat specifike të produktit dhe të përmbushin këto kërkesa për përdorimin e sigurt të produktit.

4. AOS-i të sigurojnë transportin e sigurt të produkteve në përputhje me legjislacionin për sigurinë e informacionit.

Neni 45
Kufizime

AOS-i ndalohet të përdorin në SKI produkte që nuk janë pronë e institucionit, pronë e AKSHI-t, ose për rastet e akreditimit të SKI-ve për operatorët ekonomik pronë e vetë operatorit, me përjashtim të rasteve kur ka marrëveshje sigurie me shtete dhe/ose organizata ndërkombëtare.

Neni 46
Siguria e produkteve
(Instalimi dhe konfigurimi i produkteve)

1. AOS-i të instalojnë, konfigurojnë, operojnë dhe administrojnë produktet në përputhje me kërkesat e sigurisë së produktit.

2. Institucionet shtetërore të etiketojnë produktet dhe pajisjet e TIK-ut sipas nivelit më të lartë të informacionit që trajtojnë.

3. Produktet dhe pajisjet e TIK-ut të etiketohen me numrin unik të identifikimit dhe nivelin e klasifikimit përkatës dhe të shenjëzohen me shenja dalluese sipas skemës së mëposhtme:

a) shirit portokalli – "Tepër Sekret";
b) shirit i kuq – "Sekret";
c) shirit blu – "Konfidencial";
d) shirit i bardhë – "i Kufizuar".

Neni 47
Siguria e produkteve
(Mirëmbajtja dhe riparimi i produkteve)

Mirëmbajtja dhe riparimi i produkteve dhe pajisjeve të TIK-ut të bëhet brenda zonave të sigurisë dhe nga personel i certifikuar përshtatshmërish.

Neni 48
Rastet e mirëmbajtjes në kushtet e emergjencës

Në raste emergjente, kur mirëmbajtja dhe riparimi i produkteve dhe pajisjeve të TIK është e pamundur të bëhet nga personel i certifikuar ose brenda zonave të sigurisë, institucionet shtetërore duhet të përmbushin këto detyrime:

1. Të dokumentojnë rastin dhe nevojën për një ndërhyrje të tillë.

2. Nëse është e mundur, të heqin pjesët e memories dhe të deklasifikojnë produktin ose pajisjen e TIK që do të mirëmbahet apo riparohet përpara ndërhyrjes nga persona të pacertifikuar ose jashtë zonës së sigurisë.

3. Nëse vlerësohet, të pastrohet dhe deklasifikohet produkti ose pajisja e TIK që do të mirëmbahet apo riparohet përpara ndërhyrjes për mirëmbajtje ose riparim jashtë zonës së sigurisë.

4. Personeli teknik që do të kryejë mirëmbajtjen të mbikëqyret gjatë gjithë kohës nga personel i institucionit i certifikuar dhe brifuar përshtatshmërish.

Neni 49

Pastrimi dhe nxjerrja jashtë përdorimit e pajisjeve TIK

1. Me pastrim dhe nxjerrje jashtë përdorimit të pajisjeve të TIK nënkuptohet pastrimi i komponentëve memorizues të tyre në mënyrë të pakthyeshme.

2. Komponentët memorizues brenda pajisjeve të TIK janë:

a) komponentë me memorie elektrostatike;

b) memorjet magnetike të qëndrueshme;

c) memorjet me gjysëmpërcjells;

d) memorjet e paqëndrueshme.

3. AOS-i të hartojnë procedura të mirëpërcaktuara për pastrimin e komponentëve memorizues të pajisjeve TIK përpara se t'i nxjerrin jashtë përdorimit sipas modelit të ofruar nga DSIK.

4. AOS-i të pastrojnë komponentët memorizues të pajisjeve TIK duke mbishkruar tërësisht memorien të paktën dy herë me një model të rastësishëm, ndjekur nga një rilexim për verifikim dhe nga shkëputja e energjisë për të paktën dhjetë minuta.

5. Nëse rileximi është i pamundur ose nëse në komponentët memorizues ekziston informacion i klasifikuar, ndiqen procedurat e shkatërrimit shpjeguar më poshtë.

6. Pas procedurave të pastrimit pajisjet TIK dhe komponentët e tyre memorizues trajtohen si më poshtë:

Niveli i klasifikimit para pastrimit	**Niveli i klasifikimit pas pastrimit**
Tepër Sekret	Tepër Sekret
Sekret	Konfidencial
Konfidencial	I paklasifikuar
I Kufizuar	I paklasifikuar

7. Procedurat e pastrimit iniciohen nga pajisje të tjera TIK, të ndryshme nga pajisjet që i nënshtrohen procesit të pastrimit.

8. Rast përjashtimi nga ripërdorimi në rrjet të klasifikuar është kur në komponentët memorizues të pajisjeve TIK është ruajtur çelës kriptografik statik.

Neni 50

Shkatërrimi dhe asgjësimi i pajisjeve TIK

1. AOS-i të hartojnë procedura të mirëpërcaktuara për shkatërrimin e komponentëve memorizues të pajisjeve TIK.

2. Procedura të mbikëqyret nga të paktën tre punonjës të certifikuar në nivelin e klasifikimit të pajisjeve që po i nënshtrohen kësaj procedure.

3. Të përdoret një nga metodat si në tabelë:

Produkti hardware	**Metodat e shkatërrimit**					
	Furrë djegi	**Mulli me**	**Disintegrator /Shpërbërës**	**Grirës/ Grimcues**	**Prerës**	**Degausser /**

	e	goditje				Demagnetizues
Pajisje me memorie elektrostatike	PO	PO	PO	PO	JO	JO
Floppy disk magnetik	PO	PO	PO	JO	PO	PO
Hard disk magnetik	PO	PO	PO	PO	JO	PO
Shirit magnetik	PO	PO	PO	JO	PO	PO
Disk optik	PO	PO	PO	PO	PO	JO
Memorie me gjysëmpërcjellës	PO	PO	PO	JO	JO	JO

4. Në rastet e përdorimit të pajisjes Degausser/Demagnetizues për shkatërrim, pajisja duhet të jetë e certifikuar dhe akreditуar nga DSIK-u.

5. Gjatë përdorimit të pajisjes Degausser/Demagnetizues, testohet rregullisht fuqia e fushës për të konfirmuar se procedura po kryhet konform kërkesave.

6. Të hartohen procedura të mirëpërcaktuara për trajtimin e mbetjeve të komponentëve memorizues të pajisjeve TIK pas deklasifikimit dhe shkatërrimit.

Neni 51
Siguria e aplikacioneve
(Të përgjithshme)

1. AOS-i duhet që:

a) të përdorin aplikacione të licensuara, të miratuara nga AKAS.

b) janë përgjegjës për regjistrimin, kontrollin dhe ruajtjen për arsye *backup*-i të aplikacioneve që kanë në përdorim, dhe nëse aplikohet për shenjëzimin e tyre përshtatshmërisht me nivelin e klasifikimit.

c) Të dokumentojnë në dokumentet e sigurisë së sistemit (DSS dhe/ose POS) funksionet e sigurisë së aplikacioneve, nëse aplikohet.

d) Të lejojnë transferimin manual të të dhënave ndërmjet SKI-ve nëpërmjet mediave të lëvizshme nën kontroll të rreptë dhe vetëm në rrethana kur nevojat operacionale e kërkojnë këtë transferim. Institucionet shtetërore të përcaktojnë dhe dokumentojnë procedurat e transferimit manual të të dhënave në POS të sistemit.

2. AOS-i të ndalojnë:

a) ndryshimet në konfigurimet e aplikacioneve ose në vetë aplikacionin pa aprovimin paraprak të titullarit të institucionit. Nëse këto ndryshime ndikojnë në profilin e sigurisë së sistemit, të merret paraprakisht miratimi i AKAS-ut;

b) përdorimin e autorizuar dhe të paautorizuar të SKI-ve te aksesojne sistemin duke përdorur kredenciale dhe/ose identitete të tjera;

c) përdorimin e llogarive në grup në sisteme të klasifikuar në nivel Konfidencial e lart që operojnë në mënyrën e lartë të sigurisë ose në mënyrën me shumë nivele. Në SKI-të që operojnë në mënyrën e dedikuar, mund të përdoren llogaritë në grup me kusht që të aprovohen nga AKAS-i rast pas rasti. Megjithatë, në çdo rast të merren masat përkatëse për identifikimin, autentifikimin dhe mbajtjen në llogari të individëve që aksesojnë llogaritë në grup.

Neni 52
Mjediset e operimit standard

Në mjediset e operimit standard merren masat që:

1. Të sigurojnë çaktivizimin, riemërimin ose ndryshimin e fjalëkalimeve të llogarive default të sistemeve operative.

2. Të fshijnë ose çaktivizojnë llogaritë e përdoruesve, aplikacionet, komponentët, shërbimet dhe funksionalitetet e panevojshme në sistem.

3. Të çaktivizojnë llogaritë e administratorëve lokalë dhe të përdorin llogari domaini me të drejta administrative lokale.

4. Të aktivizojnë dhe konfigurojnë funksionet e sigurisë që ofrojnë aplikacionet dhe të çaktivizojnë funksionet e panevojshme për përdoruesit.

5. Të ndjekin udhëzimet e prodhuesve, nëse ka, për konfigurimin e sigurt të produkteve të tyre.

6. Të përdorin metoda të kontrollit të aplikacioneve për kufizimin e ekzekutimit të programeve, dll-ve dhe skripteve sipas një liste të miratuar.

7. Të konfigurojnë mekanizmat e kontrollit të aplikacioneve për gjenerimin e logeve gjatë ndërhyrjeve të dështuara dhe të regjistrojnë informacion në lidhje me *file*-t e bllokuara, kohën dhe përdoruesin që tentoi të ekzekutojë *file*-n.

8. Të përdorin sisteme të parandalimit të ndërhyrjeve *host-based* në serverë që administrojnë informacion të klasifikuar në nivel "Sekret" dhe "Tepër sekret".

9. Të përdorin aplikacione *firewall software-based* për të kufizuar lidhjet hyrëse dhe dalëse të rrjetit.

10. Të përdorin aplikacione të kontrollit të pajisjeve periferike për të parandaluar përdorimin e paautorizuar të mediave kompjuterike dhe pajisjeve në kompjuterë dhe serverë.

11. Të mos lejojnë përdoruesit të çaktivizojnë ose tejkalojnë mekanizmat e kontrollit të aplikacioneve.

12. Të mos lejojnë përdoruesit të instalojnë, çinstalojnë ose çaktivizojnë aplikacione.

13. Të mos lejojnë pajisje të lidhen njëkohësisht në dy rrjete të ndryshme.

Neni 53

Mbrojtja nga aplikacionet keqdashëse dhe viruset kompjuterike

1. AOS-i duhet të përdorin programe kundër aplikacioneve keqdashëse dhe viruseve kompjuterike në sistemet e tyre dhe të dokumentojnë detajet që lidhen me to, përfshirë kërkesat dhe procedurat për përditësim dhe skanim si dhe personat përgjegjës për përditësimin e tyre dhe ndjekjen e procedurave të sigurisë.

2. AOS-i të sigurojnë që këto programe:

a) përditësohen rregullisht.

b) janë konfiguruar për skanim automatik dhe periodik të disqeve dhe mediave të lëvizshme.

3. AOS-i të dokumentojnë në POS instruksionet për veprimet që duhen ndërmarrë dhe raportimin e incidenteve që lidhen me infektimet e aplikacioneve keqdashëse dhe viruseve kompjuterike.

Neni 54

Përditësimi (*patching*) i software-ve

1. AOS-i duhet që:

a) të përfshijnë në POS procedurat e menaxhimit të përditësimeve të sistemeve operative, aplikacioneve, driverave dhe firmware-ve të pajisjeve.

b) të monitorojnë burimet e informacionit për dobësitë e reja dhe përditësimet përkatëse për sistemet operative, aplikacionet, driverat dhe firmware-t e pajisjeve.

2. Sistemet operative, aplikacionet dhe pajisjet hardware që nuk suportohen më nga prodhuesi të zëvendësohen me një version që suportohet nga prodhuesi ose me një version të suportueshëm nga një prodhues tjetër.

Neni 55
Zhvillimi i aplikacioneve

1. Gjatë zhvillimit të aplikacioneve për trajtimin e informacionit të klasifikuar, të merret në konsideratë përmbushja e objektivave të sigurisë gjatë gjithë fazave të zhvillimit të aplikacioneve (dizenjimi, zhvillimi, shpërndarja dhe mirëmbajtja).
2. Aplikacionet t'u nënshtrohen procesit të testimit të sigurisë, menaxhimit të konfigurimeve dhe kontrollit të ndryshimeve.
3. AOS-i të mos lejojnë aksesin e paautorizuar në kodin burim të aplikacioneve.

Neni 56
Implementimi i teknologjisë web në sistemet e klasifikuar

1. AOS-i të hartojnë dhe dokumentojnë procedurat për implementimin dhe përdorimin e shërbimeve intranet në sistemet e tyre.
2. AOS-i të sigurojnë që të gjithë faqet web të shenjëzohen përshtatshmërisht me nivelin më të lartë të klasifikimit të informacionit që përmbahet në atë faqe.
3. AOS-i të sigurojnë vlefshmërinë dhe/ose pastrimin e të gjithë inputit në një aplikacion web.
4. AOS-i të implementojnë kontrollet e sigurisë së browser-ave për mbrojtjen e aplikacioneve web dhe përdoruesve të tyre.

Neni 57
Sistemet e databazave

AOS-i duhet që:
1. të mirëmbajnë dhe monitorojnë rregullisht inventarin e saktë të databazave që kanë në zotërim dhe përmbajtjeve të tyre.
2. Të fshijnë të gjithë skedarët dhe loget e përkohshme të instalimit pas instalimit të sistemeve për menaxhimin e databazave.
3. Të konfigurojnë në mënyrë të sigurt sistemet e menaxhimit të databazave në përputhje me udhëzimet e prodhuesit.
4. Të fshijnë të gjithë databazat model që instalohen me sistemin e menaxhimit të databazave.
5. Të konfigurojnë sistemin e menaxhimit të databazave të funksionojë nën një llogari të veçantë përdoruesi me minimumin e privilegjeve që nevojiten për kryerjen e funksioneve. Kjo llogari të ketë akses të kufizuar në zona joesenciale të sistemit të skedarëve të serverit të databazës.
6. Të sigurojnë ruajtjen e fjalëkalimeve të kriptuara me algoritma të fortë kriptimi në databaza.
7. Të aplikojnë kontrolle aksesi në skedarët e databazave.
8. Të kriptojnë harddisqet e serverave të databazave plotësisht (*full disk encryption*).
9. Të shenjëzojnë përshtatshmërisht databazat ose përmbajtjet e tyre.
10. Të ndajnë privilegjet e përdoruesve të databazës sipas nevojës për njohje duke u dhënë atyre privilegjet e nevojshme për akses, futje të dhënash, modifikim ose fshirje të dhënash në databazë sipas detyrave përkatëse.
11. Të çaktivizojnë, riemërojnë ose ndryshojnë fjalëkalimet e llogarive default të administratorëve të databazave.
12. Të sigurojnë që administratorët e databazave të kenë llogari unike dhe të identifikueshme për secilin administrator.

13. Të sigurojnë që llogaritë e administratorëve të databazave të përdoren ekskluzivisht për detyra administrative.

14. Të sigurojnë që administratorëve të databazave t'u jepet akses sipas roleve që kanë dhe jo të gjitha të drejtat ose të drejtat default të administratorëve.

15. Të fshijnë llogaritë anonime të databazave.

16. Serverët e databazave dhe serverët web të ndahen funksionalisht, nëpërmjet një ndarje fizike ose virtuale.

17. Të vendosin serverët e databazave në një segment rrjeti të ndryshëm nga kompjuterët e përdoruesve.

18. Të implementohen kontrollet e aksesit të rrjetit për të kufizuar komunikimet e serverëve të databazave me pjesët e tjera të rrjetit sipas një skeme të mirëpërcaktuar.

19. Të filtrojnë të gjithë pyetësorët (*queries*) nga aplikacionet web në sistemet e databazave për përmbajtje të ligjshme dhe sintaksë korrekte.

20. Të përdorin pyetësorë me parametra të caktuar ose procedura të ruajtura në vend të pyetësorëve të gjeneruar automatikisht.

21. Të kriptohet informacioni që komunikohet ndërmjet sistemeve të databazave dhe aplikacioneve web.

22. Të dizenjojnë aplikacione web që të ofrojnë sa më pak informacion të sistemit të menaxhimit të databazave dhe skemave të databazave për përdoruesit gjatë gabimeve që mund të ndodhin në sistem.

23. Të mos lejojnë ose fshijnë të gjithë funksionet dhe procedurat e ruajtura të panevojshme të sistemeve për menaxhimin e databazave.

24. Të mos lejojnë opsionet e sistemit të menaxhimit të databazave për leximin e filave lokale nga serveri.

25. Të mos kryejnë aktivitete testimi dhe zhvillimi të databazave në serverët e databazave në përdorim.

26. Të mos përdorin informacion të klasifikuar në mjediset e testimit dhe zhvillimit të databazave, përveç nëse janë akreditуar përshtatshmërish me nivelin më të lartë të informacionit që trajtojnë.

Neni 58

Siguria e e-mail-eve
(Posta elektronike)

AOS-i që kërkojnë të implementojnë shërbimet e postës elektronike në sistemet e klasifikuara duhet:

1. Të sigurojnë që infrastruktura e postës elektronike të jetë pjesë e sistemit të klasifikuar dhe të mos ketë lidhje me sisteme të tjera të paakredituara përshtatshmërish.

2. Të hartojnë procedura për përdorimin e sigurt të postës elektronike të klasifikuar.

3. Të implementojnë masat e nevojshme që sigurojnë ndjekjen e këtyre procedurave.

4. Të shenjëzojnë mesazhet e postës elektronike në përputhje me nivelin e informacionit që mezazhi përmban dhe nivelin e informacionit të dokumenteve bashkëlidhur, nëse ka.

Neni 59

Kontrolli i aksesit

1. AOS-i të implementojnë dhe dokumentojnë procedurat për identifikimin, autentifikimin dhe autorizimin e çdo entiteti (person, pajisje apo shërbim) që ka qasje në sistem apo informacionin e klasifikuar që trajtohet në të.

2. AOS-i të sigurojnë që çdo përdorues:

a) Të identifikohet në mënyrë unike.

b) Të autentifikohet në çdo rast që i miratohet qasja në sistem.

c) Të autorizohet sipas parimit "nevojë për njohje".

3. AOS-i, të cilat përdorin fjalëkalimin si të vetmen metodë autentifikimi, të implementojnë një nga politikat e mëposhtme:

a) fjalëkalimi të jetë i përbërë nga minimalisht 13 karaktere jo kompleks

b) fjalëkalimi të jetë i përbërë nga minimalisht 10 karaktere dhe në përbërje të ketë shkronja te vogla, shkronja të mëdha, numra dhe karaktere specifike (të paktën një prej secilit tip në çfarëdolloj renditje).

4. Për sistemet ku trajtohet informacion i klasifikuar në nivel "Tepër Sekret" AOS të implementojnë një nga politikat e mëposhtme:

a) Fjalëkalimi të jetë i përbërë nga minimalisht 15 karaktere jo kompleks

b) Fjalëkalimi të jetë i përbërë nga minimalisht 11 karaktere dhe në përbërje të ketë shkronja te vogla, shkronja të mëdha, numra, karaktere specifike.

5) AOS-i, në varësi të rezultateve të raportit të vlerësimit të riskut, të implementojnë një metodë të kombinuar autentifikimi për përdoruesit e privilegjuar si:

a) administrator sistemi;

b) administrator database-i;

c) përdorues me të drejta jo të kufizuara;

d) përdorues me të drejta të Aksesit në largësi;

e) përdorues.

6. AOS të ndjekin praktikën e mëposhtme për menaxhimin e fjalëkalimeve:

a) të sigurojnë që fjalëkalimet të ndryshohen çdo 90 ditë.

b) të parandalojnë ndryshimin e fjalëkalimeve nga përdoruesit më shumë se një herë në ditë.

c) të parandalojnë përdorimin e të njëjtit fjalëkalim në vazhdimësi. I njëjti fjalëkalim mund të përdoret vetëm pas 8 fjalëkalimesh të ndryshme.

d) të parandalojnë ruajtjen e fjalëkalimeve në tekst të hapur.

e) të bllokojnë llogarinë e përdoruesit pas maksimumi 5 përpjekjesh të dështuara për akses/qasje në llogari.

f) të dokumentojnë dhe implementojnë mënyrat e rivendosjes (riset) së fjalëkalimeve pas bllokimit të aksesit/qasjes në llogari.

g) gjatë aktivizimit të llogarisë për herë të parë, përdoruesit t'i vihet në përdorim një fjalëkalim "i përdorshëm vetëm një herë" dhe të detyrohet të ndryshojë fjalëkalimin gjatë logimit në sistem.

7. AOS-i të dokumentojnë dhe implementojnë procedurat për mbylljen e sesionit apo ekranit.

8. AOS-i të fshijnë ose pezullojnë llogaritë e përdoruesve në të njëjtën ditë që përdoruesit nuk kanë ligjërisht të drejta aksesi/ qasje në sistem.

9. AOS-i të implementojnë banera logimi ku të informojnë përdoruesit mbi të drejtat që kanë në sistem, përgjegjësit dhe detyrimet ligjore.

Neni 60

Auditimi dhe ruajtja e logeve të sigurisë

1. AOS të hartojnë dhe implementojnë procedurat për ruajtjen dhe auditimin e log-eve.

2. Institucionet shtetërore të ruajnë minimalisht ngjarjet që lidhen me:

a) veprimet e privilegjuara;

b) shtimin, fshirjen dhe modifikimin e të drejtave të aksesit të përdoruesve dhe grupeve;

c) përpjekjet e dështuara për akses/qasje në sisteme dhe file kritike;

d) paralajmerime (alert) dhe dështime që lidhen me sigurinë e sistemit;

e) hyrjet/daljet në sistem;

f) përpjekjet e dështuara për hyrje në sistem.

3. Për çdo ngjarje të ruhet:

a) data dhe ora e ngjarjes.

b) përdoruesi apo procesi që lidhet me ngjarjen.

c) përshkrim i ngjarjes.

d) dështim apo suksesi i ngjarjes.

e) burimi i ngjarjes (p.sh. emri i aplikacionit).

f) vendndodhja/ identifikimi i pajisjes ku ka ndodhur.

4. Këto rekorde të ruhen sipas një periudhe të rënë dakord ndërmjet AKAS dhe AOS të specifikuar në DSS dhe POS përkatëse. Për informacionin e klasifikuar në nivel "Tepër sekret" kjo periudhë të jetë minimalisht 5 vjet.

5. Informacioni i auditimit të mbrohet nga aksesi, ndryshimi ose fshirja e paautorizuar.

6. Anomalitë dhe incidentet e sigurisë të raportohen tek AKAS-i.

Neni 61

Menaxhimi i rrjetit

1. AOS-i duhet që:

a) të menaxhojnë rrjetet në mënyrë të përqendruar.

b) të dokumentojnë dhe aprovojnë të gjitha ndryshimet në konfigurimet e rrjetit.

c) Të kontrollojnë vazhdimisht përputhjen e konfigurimeve të rrjetit me konfigurimet e dokumentuara.

2. Dokumentacioni i konfigurimeve/rrjetit të përfshijë:

a) diagramin e rrjetit ku tregohen të gjitha lidhjet e rrjetit;

b) diagram logjike të rrjetit ku tregohen të gjitha pajisjet e rrjetit, shërbimet dhe serverët;

c) konfigurimet e pajisjeve të rrjetit.

3. Dokumentacioni i konfigurimeve/rrjeti të përditësohet me ndryshimet e fundit dhe të klasifikohet në tërësi me nivelin më të lart të informacionit që trajtohet në rrjet.

4. Dokumentacioni i rrjetit që u vihet në dispozicion palëve të treta të përmbajë vetëm detajet e nevojshme për përmbushjen e detyrimeve, shërbimeve sipas kontratës.

5. AOS-i të inventariziojnë pajisjet e rrjetit, të përditësojnë dhe auditojnë inventarin rregullisht.

Neni 62

Dizenjimi dhe konfigurimi i rrjetit

1. AOS-i të implementojnë kontrollet mbi aksesimin e rrjetit për të kufizuar trafikun sipas nevojës për njohje brenda dhe ndërmjet segmenteve të rrjetit.

2. Në rastet kur informacioni i klasifikuar procesohet, ruhet apo komunikohet nga sisteme të cilat nuk janë në kontroll të institucionit, ai duhet të sigurojë që pala tjetër ka aplikuar masat e duhura të sigurisë në përputhje me këtë rregullore.

3. AOS-i:

a) të çaktivizojnë portat fizike të pa përdorura në pajisjet e rrjetit.

b) të çaktivizohen, riemërtohen ose të ndryshohen fjalëkalimet të tyre llogarive *default* në pajisjet e rrjetit.

c) të sinkronizohet koha në të gjitha pajisjet e rrjetit.

4. AOS-i të zhvillojnë, implementojnë, mirmbajnë procedurat e sistemit të dedektimit dhe parandalimit të ndërhyrjeve ku të përfshijnë:

a) sistemet NISP, NISD;

b) procedura dhe burime për mirëmbajtjen dhe kontrollin e nënshkrimeve elektronike;

c) procedura dhe burime për analizimin e logeve dhe alerteve në kohë reale;

d) procedura dhe burime për përgjigje ndaj incidenteve të dedektuara (zbuluara);

e) frenkuencat e rishikimit të procedurave dhe burimeve të dedektimit(zbulimit) dhe parandalimit.

5. AOS-i në rastet e ndërlidhjes së sistemeve të aplikojnë sistemet e detektimit dhe parandalimit të ndërhyrjeve në të gjitha nyjat e ndërlidhjes.

6. Lejohet përdorimi i VLAN-eve për ndarjen e trafikut të rrjetit vetëm ndërmjet rrjeteve në të njëjtin nivel klasifikimi.

7. Të përdoren funksionet IPv6 kur është e mundur, në të kundërt t'i çaktivizojnë funksionet IPv6 në të gjitha pajisjet e sistemit.

8. Në sistemet e klasifikuara ndalohet rreptësish përdorimi i pajisjeve *wireless*.

Neni 63

Videokonferencat, rrjeti telefonik dhe telefonia IP

1. Institucionet shtetërore në rastet e përdorimit të video konferencave dhe telefonisë IP të klasifikuar:

a) të marrin masa për kriptimin e të dhënave.

b) të kryejnë autentifikimin dhe autorizimin për të gjitha veprimet në rrjetin e video konferencave dhe telefonisë IP.

2. Telefonia IP të konfigurohet në mënyrë të tillë që:

a) telefonat IP të autentifikojnë vetveten te menaxhuesi i thirrjeve gjatë regjistrimit;

b) të çaktivizohet funksioni i vetëregjistrimit të pajisjeve dhe të lejohet aksesi në rrjet vetëm për një listë të mirëpërcaktuar të pajisjeve të autorizuara;

c) të bllokohen pajisjet e paautorizuara;

d) të çaktivizohen funksionet e papërdorura dhe të ndaluara.

3. Trafiku i videokonferencave dhe telefonisë IP të ndahet fizikisht ose logjikisht nga trafiku i të dhënave të tjera të rrjetit.

4. Në zonat e sigurisë ndalohet përdorimi i mikrofonave, kufjeve, receptorëve USB dhe kamerave web.

KREU V

SIGURIMI KRIPTOGRAFIK

Neni 64

Të përgjithshme

1. Institucionet shtetërore të përdorin produkte, algoritma dhe/ose protokolle kriptografike të vlerësuara nga Autoriteti Kombëtar i Sigurimit të Komunikimeve dhe të miratuara nga DSIK për kriptimin e informacionit të klasifikuar "Sekret shtetëror" të palëvizshëm ose në transit.

2. DSIK-u mban listën e produkteve, algoritmeve dhe protokolleve kriptografike të miratuar për përdorim.

3. institucionet shtetërore për kriptimin e të dhënave të palëvizshme të përdorin;

a) kriptimin e plotë të diskut.

b) Kriptimin e pjesshëm të diskut me kusht që të lejohet shkrimi vetëm në particione të kriptuara.

4. Produktet kriptografike të ofrojnë një mënyrë për rikuperimin e të dhënave në rast të humbjes ose dëmtimit të çelësit kriptografik, kur është e mundur.

5. Institucionet shtetërore të përdorin kriptimin e të dhënave në transit në rastet kur informacioni i klasifikuar shkëmbehet nëpërmjet infrastrukturës së rrjeteve publike ose rrjeteve me nivel më të ulët të klasifikimit.

Neni 65

Menaxhimi i materialit kriptografik

Institucionet shtetërore duhet që:

1. Të shpërndajnë, menaxhojnë dhe ruajnë pajisjet dhe materialet kriptografike sipas rregullave dhe procedurave të specifikuara me rregullore të veçantë.

2. Të hartojnë Planin e Menaxhimit të Materialit Kriptografik kur implementojnë sisteme kriptografike që përdorin pajisje kriptografike.

3. Të ruajnë pajisjet dhe materialet kriptografike në zona të sigurisë së klasit I.

4. Të mbajnë dhe përditësojnë regjistrin e aksesit në të cilin të ruhet informacion në lidhje me sistemin kriptografik, si:

a) detaje të personelit që ka akses në sistem në nivel administratori;

b) detaje të personelit që i është hequr aksesi në system në nivel administratori;

c) detaje të dokumentave të sistemit;

d) aktivitetet e mbajtjes në llogari të transaksioneve me pajisjet dhe materialet kriptografike;

e) aktivitetet e kontrollit të sigurisë së sistemit.

5. Përpara dhënies së aksesit personelit për sigurinë e komunikimeve të sigurojnë që personat:

a) të kenë nevojën për akses;

b) të lexojnë dhe pranojnë Planin e Menaxhimit të Materialit Kriptografik për sistemin kriptografik që përdorin;

c) të jenë të pajisur me certifikatë të përshtatshme të sigurisë së personelit;

d) të mbrojnë dhe të mos nxjerrin informacionin e autentifikimit të sistemit kriptografik;

e) të pranojnë të mbajnë përgjegjësi për të gjitha veprimet nën llogarinë e tyre;

f) të raportojnë problemet që lidhen me sigurinë në instancat e duhura.

6. Të mbajnë në llogari të gjitha transaksionet që lidhen me materialet e sistemit kriptografik, përfshirë pjesët *hardware* dhe *software* të lëshuara me pajisjet dhe materialet kriptografike, kur janë lëshuar dhe ku.

7. Të inventarizojnë materialin e sistemit kriptografik:

a) gjatë kalimit të përgjegjësive administrative (dorëzimit/marrjes të detyrës) për sistemin kriptografik;

b) gjatë ndryshimit të personelit që ka akses në sistemin kriptografik;

c) të paktën 2 herë në vit;

8. Të kryejnë kontroll të inventarit për të verifikuar nëse materialet e sistemit kriptografik janë në përputhje me dokumentacionin.

9. Të sigurojnë që kontrolli i inventarit të kryhet nga persona të trajnuar për aspektet e sigurisë së komunikimeve.

10. Të anulojnë materialet çelës ose certifikatat nëse dyshohet se janë kompromentuar.

11. Të raportojnë te DSIK për çdo material çelës ose certifikatë që dyshohet se është kompromentuar.

KREU VI
SIGURIA E NDËRLIDHJES SË SISTEMEVE TË KLASIFIKUAR

Neni 66
Të përgjithshme

Për çdo ndërlidhje të SKI-ve, zbatohen kërkesat sa më poshtë:

1. Kërkesat operacionale dhe funksionale të ndërlidhjes të jenë miratuar nga zotëruesit e SKI-ve.

2. Ndërlidhja e SKI-ve kalon në procesin e akreditimit të sigurisë.

3. Të kalojë procesin e vlerësimit, certifikimit dhe/ose të aprovimit të mekanizmave me funksione sigurie nga AKAS.

4. Ndalohet ndërlidhja e SKI-ve që trajtojnë informacion të klasifikuar në nivel "Tepër sekret".

5. SKI-të që trajtojnë informacion të klasifikuar mund të përdorin internetin ose rrjetet e ngjashme të domain-it publik vetëm si bartëse, me kusht që në to të implementohet mbrojtja e duhur kriptografike.

6. Ndalohet ndërlidhja e SKI-ve në kaskadë.

7. Ndalohet ndërlidhja e SKI-ve me rrjete të paklasifikuara, me përjashtim të rastit të SKI-ve në nivel "i Kufizuar".

Neni 67

Pajisjet *gateway*

1. AOS të sigurojnë që:

a) Sistemet të mbrohen nga sistemet e *domain*-eve të tjera me një ose më shumë pajisje *gateway*.

b) Pajisjet *gateway* të përmbajnë mekanizma për filtrimin e rrjedhës së të dhënave në shtresën e rrjetit (nivel rrjeti).

c) Të gjitha lidhjet ndërmjet *domain*-eve të sigurisë të përmbajnë mekanizma për inspektimin dhe filtrimin e rrjedhës së të dhënave për shtresën e transportit dhe më lart sipas modelit OSI.

2. AOS të sigurojnë që pajisjet *gateway*:

a) janë të vetmet rrugë komunikimi ndërmjet rrjeteve;

b) në gjendje *default*, të pengojnë të gjithë lidhjet brenda dhe jashtë rrjetit;

c) lejojnë vetëm lidhjet e autorizuara në mënyrë eksplicite;

d) janë konfiguruar me masat e përshkruara në këtë rregullore;

e) menaxhohen nëpërmjet një pathi të sigurt të izoluar nga rrjetet e lidhura (fizikisht me *gateway* ose në një rrjet administrues të dedikuar);

f) ofrojnë regjistrim logesh dhe kapacitete të mjaftueshme për Identifikimin e incidenteve të sigurisë kompjuterike, përpjekjet për ndërhyrje dhe *pattern*-e të përdorimit të pazakontë

g) ofrojnë alerte në kohë reale.

3. AOS-i duhet që:

a) të përdorin zonat e demilitarizuara (DMZ) për ofrimin e shërbimeve që aksesohen nga autoritetet e tjera të ndërlidhur;

b) të kryejnë vlerësimin e riskut të sigurisë në pajisjet *gateway* dhe konfigurimet përkatëse përpara implementimit të tyre dhe të kuptojnë e pranojnë riskun e mbetur;

c) të dokumentojnë dhe vlerësojnë të gjitha ndryshimet në arkitekturën e pajisjeve *gateway*;

d) të kufizojnë aksesin në funksionet administrative të pajisjeve *gateway*;

e) të sigurojnë që administratorët janë trajnuar për menaxhimin e pajisjeve *gateway*;

f) të autentifikojnë përdoruesit dhe pajisjet e SKI në rrjetet e klasifikuar që aksesohen nëpërmjet pajisjeve *gateway*;

g) të sigurojnë që vetëm përdoruesit e autentifikuar dhe të autorizuar në një pajisje *gateway* mund ta përdorin atë;

h) të sigurojnë që të gjitha ruhen loget e të gjitha veprimeve (*events*).

Neni 68

Pajisjet *firewall*

AOS-i të përdorin pajisje *firewall* si pjesë e infrastrukturës së ndërlidhjes së sistemeve në të gjitha pikat e ndërlidhura, në mënyrë të pavarur.

Neni 69

Diodat e të dhënave

1. Në ndërlidhje sistemesh njëdrejtimësh ndërmjet rrjeteve të klasifikuar të përdoren dioda të dhënash sipas një liste të njohur sipas standardeve kombëtare, të NATO-s, BE-së dhe të certifikuar me nivelin me të lartë të informacionit i cili trajtohet në këto SKI.

2. AOS-i të monitorojnë volumin e të dhënave që transferohet në diodat e të dhënave.

Neni 70

Përmbajtjet dhe lidhjet web

AOS-i, në rastin e implementimit të faqeve web në rrjetet e klasifikuara duhet:

1. Të hartojnë politikën e përdorimit të sigurt të web-it.

2. Të sigurojnë që aksesi i web-it të kryhet nëpërmjet një web proxy.

3. Të sigurojnë që web proxy të autentifikojë përdoruesit dhe të ruajë loget me detajet e website-ve që aksesohen:

a) adresa URL.

b) koha/data.

c) përdoruesi.

d) sasia e të dhënave të upload-uara dhe download-uara.

e) adresa IP.

Neni 71

Pajisjet KVM switch

1. AOS-i të përdorin pajisje KVM switch sipas një listë të njohur sipas standardeve kombëtare, te NATO-s , BE-së për aksesimin e sistemeve sipas rasteve:

a) sistem i klasifikuar dhe sistem i paklasifikuar;

b) sisteme me nivele të ndryshme klasifikimi;

c) sisteme në të njëjtin nivel klasifikimi por në *domaine* të ndryshme.

2. Pajisjet KVM switch duhet:

a) të operohen manualisht;

b) të kenë të ndarë përshtatshmërish dhe në mënyrë të dukshme kabllot nga sisteme të ndryshme;

c) të përmbajë tregues për të njoftuar përdoruesin në rastet kur kalohet në sisteme të paklasifikuar;

d) të inspektohen rregullisht lidhur me mirëfunksionimin e tyre.

3. Pajisjet KVM switch nuk duhet të kenë procesor ose memorje të brendshme.

4. Pajisjet KVM switch nuk lejohet te lidhen me sisteme te paklasifikuara te cilat kanë konvertues Analog-Dixhital.

Neni 72

Politika dhe procedurat e transferimit të të dhënave

AOS-i të sigurojnë që:

1. Veprimet e përdoruesve që shkëmbejnë të dhëna ndërmjet sistemeve të ruhen në log-e.

2. Përdoruesit të parandalojnë incidentet kompjuterike nëpërmjet:

a) kontrollit të shenjëzimeve për të siguruar që sistemi destinacion është i përshtatshëm për administrimin e të dhënave që transferohen;

b) kryerjen e kontrollit kundër viruseve në të dhënat që transferohen;

c) ndjekjen e proceseve dhe procedurave për transferimin e të dhënave.

3. Të dhënat e importuara në sistem duhet:

a) të skanohen për përmbajtje keqdashëse dhe aktive;

b) të kontrollohet formati i të dhënave;

c) të ruhen loget për çdo ngjarje;
d) të monitorohen për identifikimin e modeleve të pazakonta të përdorimit.
4. Të dhënat e eksportuara në sistem:
a) të kontrollohen për shenjëzimet përkatëse;
b) të ruhen loget për çdo ngjarje;
c) të monitorohen për identifikimin e modele të pazakonta të përdorimit;
d) të kontrollohet formati i të dhënave;
e) të bëhen kontrolle të fjalëve;
f) të ketë procedura për kontrollin e madhësisë së skedarëve.
5. Transferimi i të dhënave të kryhet në përputhje me procedurat e miratuara të institucionit.

KREU VII
PUNA JASHTË ZONAVE TË SIGURISË

Neni 73
Pajisjet e lëvizshme

AOS-i të kryejnë veprimet e mëposhtme:
1. Të dokumentojnë procedurat e përdorimit të sigurt të pajisjeve të lëvizshme.
2. Të vlerësojnë dhe dokumentojnë riskun që lidhet me përdorimin e pajisjeve të lëvizshme.
3. Të kriptojnë informacionin që administrohet në pajisjet e lëvizshme me një produkt kriptografik të akreditуar.
4. Në rast të përdorimit të pajisjeve të lëvizshme për komunikimin e informacionit të klasifikuar mbi infrastrukturën e rrjeteve publike, të përdorin produkte kriptografike të akreditуar për kriptimin e këtij informacioni.
5. Në rast të lejimit të pajisjeve të lëvizshme për aksesimin e informacionit të klasifikuar të ndalojnë instalimin dhe çinstalimin e aplikacioneve nga përdoruesit.
6. Në rast të lejimit të pajisjeve të lëvizshme për aksesimin e informacionit të klasifikuar mos lejohet çaktivizimin e funksioneve të sigurisë nga përdoruesit.
7. Në rast të përdorimit të sistemeve nëpërmjet lidhjeve VPN të çaktivizohet *split tunnelling* në pajisjet që e suportojnë këtë funksionalitet.
8. Në rast se ofrohet funksion i zerimit ose sanitizimit të çelësave kriptografikë në pajisjet e lëvizshme, ky funksion të përdoret si pjesë e procedurave të asgjësimit në raste emergjence.
9. Të mos lejojnë përdorimin e pajisjeve të lëvizshme për përpunimin ose ruajtjen e informacionit të klasifikuar në nivel "Tepër sekret" përveçse me miratim të DSIK-së.
10. Të mos lejojnë pajisjet e lëvizshme që nuk janë në zotërim të institucionit për aksesimin dhe/ose administrimin e informacionit të klasifikuar.
11. Të mos lejojnë futjen e pajisjeve të lëvizshme që nuk janë në zotërim të institucionit pa autorizimin me shkrim të titullarit të institucionit.
12. Të mos lejojnë funksionet *bluetooth*, *wireless* apo *infrared* në pajisjet e lëvizshme.

Neni 74
Pajisjet e lëvizshme jashtë zonave të sigurisë

Për pajisjet e lëvizshme jashtë zonave të sigurisë, AOS-i të kryejë veprimet e mëposhtme:
1. Të sigurojnë që pajisjet e lëvizshme transportohen në mënyrë të sigurt jashtë zonave të sigurisë pas autorizimit të AOS-it.
2. Pajisjet e lëvizshme jashtë zonave të sigurisë të mbahen nën mbikëqyrje të vazhdueshme.
3. Personeli që udhëton jashtë shtetit me pajisje të lëvizshme:
a) të aplikojë patch-et e aplikacioneve dhe sistemeve operative;
b) të implementojë autentifikim multifaktorial;

c) të kryejë back-up-in e të dhënave;
d) të heqë informacionet e panevojshme nga pajisja;
e) të çaktivizojë aplikacionet që nuk janë të rëndësishme për periudhën e udhëtimit;
f) të çaktivizojë lidhjet bluetooth, wireless dhe infrared;
g) t'i mbajë ato nën kontroll gjatë gjithë kohës.

KREU VIII
INCIDENTET E SIGURISË KOMPJUTERIKE DHE PROCEDURAT E RAPORTIMIT

Neni 75
Përgjigja ndaj incidenteve të sigurisë kompjuterike

1. Institucionet shtetërore të zhvillojnë, implementojnë dhe mirëmbajnë mjete dhe procedura për Identifikimin dhe raportimin e incidenteve të sigurisë së sistemeve.
2. Për trajtimin e incidenteve të sigurisë të caktohet personel me kualifikimin e duhur profesional.
3. Incidentet që lidhen me sigurinë e sistemeve të regjistrohen në regjistër të veçantë. Në këto regjistra të regjistrohen minimalisht të dhënat e mëposhtme:
a) data e verifikimit të incidentit të sigurisë;
b) data kur ka ndodhur incidenti i sigurisë;
c) një përshkrim i incidentit të sigurisë, përfshirë personelin dhe mjediset e përfshira;
d) veprimet e marra;
e) kujt i është raportuar incidenti;
f) dokumenti referencë i përfshirë në incident (nëse ka të tillë).
4. Incidentet që lidhen me sigurinë e sistemeve të raportohen në strukturat e duhura me qëllimin përgjigjen, hetimin dhe inspektimin në përputhje me legjislacionin për sigurinë e SKI-ve.

Neni 76
Njoftimi i DSIK për incidentet

Kushtet në të cilat DSIK duhet njoftuar menjëherë pas ndodhjes së incidentit janë:
1. Thyerjet e sigurisë që prekin informacionin e klasifikuar.
2. Përhapje e paautorizuar e informacionit në mediat publike ose entitete të tjera.
3. Akses i paautorizuar i të dhënave.
4. Dyshime për spiunazh, sabotazh ose terrorizëm.
5. Aktivitete të brendshme keqdashëse (p.sh., kërcënim i brendshëm).
6. Incidente që përfshijnë akses të privilegjuar në SKI.
7. Incidente që përfshijnë elemente kriptografikë.
8. Incidente që cenojnë sigurinë kombëtare.

Neni 77
Operatorët ekonomikë

1. Operatorët ekonomikë/kontraktorët gjatë realizimit të kontratave të klasifikuara të përdorin SKI të akredituara përshtatshmërisht.
2. Periudha e vlefshmërisë së akreditimit është në përputhje me afatet e zbatimit të kontratës së klasifikuar, por jo më tepër se 3 vjet.
3. Për operatorët ekonomikë ndalohet akreditimi i SKI-ve në nivel "Tepër sekret" ose ekuivalent.
4. Ndalohet ndërlidhja e SKI-ve për operatorët ekonomik/kontraktorët me SKI të institucioneve shtetërore.

Neni 78

Dispozita kalimtare dhe të fundit

1. Ministritë, institucionet shtetërore dhe Operatorët Ekonomik/Kontraktorët të marrin masa për zbatimin e kërkesave të kësaj rregulloreje.

2. Ngarkohet Drejtoria e Sigurimit të Informacionit të Klasifikuar për kontrollin e zbatimit të kërkesave të kësaj rregulloreje.

3. Ngarkohet Drejtoria e Sigurimit të Informacionit të Klasifikuar dhe Drejtoria e Shifrës për ngritjen e autoriteteve përkatëse brenda vitit 2020.

4. Institucionet shtetërore të cilat nuk përmbushin standardet e sigurisë për ngritjen e strukturave të parashikuara në këtë vendim, të marrin masat për arritjen e standardeve brenda 2021.

5. Ministritë, institucionet shtetërore dhe operatorët ekonomikë, duhet që brenda 90 ditëve nga hyrja në fuqi e këtij vendimi, të nxjerrin udhëzimet përkatëse për zbatimin e tij.

6. Vendimi 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)", shfuqizohet.

Neni 79

Hyrja në fuqi

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.