PËR INFORMACIONIN E KLASIFIKUAR

Baza Ligjore:

1. Ligji Nr. 10/2023 "Për informacionin e klasifikuar";
2. Vendim nr. 792, datë 28.12.2023 "Për miratimin e rregullores "Për përcaktimin e rregullave dhe të procedurave për sigurinë e informacionit të klasifikuar, që trajtohet në sistemet e komunikimit dhe informacionit (SKI)"";
3. Vendim nr. 659, datë 23.10.2024 "Për miratimin e rregullores "Për sigurinë industriale, rregullat, procedurat dhe kërkesat për mbrojtjen e informacionit të klasifikuar gjatë prokurimit në fushën e mbrojtjes dhe të sigurisë"";
4. Vendim nr. 731, datë 27.11.2024 "Për miratimin e rregullores "Për sigurinë e personelit"";
5. Vendim nr. 822, datë 26.12.2024 "Për miratimin e rregullores "Për klasifikimin, punën, transportimin fizik, deklasifikimin, zhvlerësimin, asgjësimin dhe shkatërrimin e informacionit të klasifikuar "sekret Shtetëror", të NATO-s, të Bashkimit Evropian, të shteteve dhe organizatave të tjera ndërkombëtare"";
6. Vendim nr. 823, datë 26.12.2024 "Për miratimin e rregullores "Për sigurimin fizik të informacionit të klasifikuar "sekret Shtetëror", të NATO-s, të Bashkimit Evropian, të shteteve dhe organizatave të tjera ndërkombëtare"".

Këshilla të përgjithshme:

- Informacioni i klasifikuar administrohet, përpunohet dhe diskutohet vetëm brenda Zonave të Sigurisë e sipas standardeve të sigurisë fizike.
- Ndalohet aksesi tek informacioni i klasifikuar jashtë këtyre mjediseve.
- Informacioni i klasifikuar përpunohet vetëm në pajisje/sisteme të akredituara përshtatshmërisht më parë nga AKSIK.
- Ndalohet aksesi tek informacioni i klasifikuar në pajisje/sisteme të paakredituara.
- Mos mbani telefonat celularë në mjedise ku diskutohet, përpunohet apo administrohet informacion i klasifikuar.
- Fjalëkalimet e kompjuterëve, kombinimet e kasafortave ku mbahet informacion i klasifikuar dhe çelësat e zyrave brenda Zonave të Sigurisë, duhet të administrohen e mbahen vetëm nga personi/personat e autorizuar nga titullari institucionit.
- Mbyllni kompjuterin kur dilni nga zyra qoftë edhe për pak kohë.
- Mos i jepni askujt çelësat e zyrës. Depozitoni kopjen e tij sipas rregullave të përcaktuara nga Titullari i institucionit.
- Mos mbani informacion të klasifikuar mbi tavolinën e punës në përfundim të orarit zyrtar.
- Sigurohuni që "CSP" është gjithnjë e vlefshme, filloni rinovimin e saj pesë muaj përpara datës së mbarimit të afatit të vlefshmërisë.
- Raportoni çdo shkelje apo incident sigurie tek Oficeri i Sigurisë/Struktura e Sigurisë/OSAK/OSIP/OSI.

Pyetje të shpeshta:

I. SIGURIA E INFORMACIONIT

1. Çfarë quajmë "informacion të klasifikuar" ?

Informacioni i klasifikuar "sekret shtetëror" është çdo dokument ose material, pavarësisht nga forma dhe natyra e tij, i përgatitur ose që përgatitet, të cilit i është vendosur një nivel i caktuar klasifikimi dhe afat ruajtjeje klasifikimi në përputhje me ligjin Nr. 10/2023 "Për informacionin e klasifikuar", në interes të sigurisë kombëtare dhe mbrohet nga shkatërrimi, humbja, vjedhja, rrjedhja, përhapja e paautorizuar ose qasja nga çdolloj tjetër kompromet imi sigurie.

2. Çfarë kuptojmë me siguri të informacionit të klasifikuar?

Me siguri të informacionit të klasifikuar kuptojmë tërësinë e procedurave dhe standardeve që garantojnë sigurinë e informacionit të klasifikuar gjatë procesit të krijimit, administrimit dhe mbikëqyrjes së tij.

3. Cilat janë nivelet e klasifikimit?

Informacioni i klasifikuar "sekret shtetëror", në bazë të përmbajtjes, të vlerave dhe interesit shtetëror, klasifikohet në njërin nga katër nivelet e mëposhtme:
a) "Tepër sekret", kur ekspozimi i paautorizuar mund t'i shkaktojë dëme jashtëzakonisht të rënda sigurisë kombëtare;
b) "Sekret", kur ekspozimi i paautorizuar mund t'i shkaktojë dëme serioze sigurisë kombëtare;
c) "Konfidencial", kur ekspozimi i paautorizuar mund t'i shkaktojë dëme sigurisë kombëtare;
ç) "I kufizuar", kur ekspozimi i paautorizuar mund të dëmtojë veprimtarinë ose efektivitetin e institucioneve të administratës publike në fushën e sigurisë kombëtare.

4. Kur ndalohet klasifikimi i një informacioni?

Ndalohet klasifikimi i një informacioni kur ai bëhet me qëllim që:
a) të fshehë moszbatimin e ligjeve, paefektshmërinë apo gabimet e administratës publike;
b) t'i privojë të drejtën e njohjes një individi, personi fizik a juridik, publik a privat;
c) të pengojë apo të vonojë dhënien e informacionit që nuk kërkon mbrojtje në interes të sigurisë kombëtare.

5. Cilët janë autoritetet klasifikuese?

1. Autoritete klasifikuese të drejtpërdrejta në Republikën e Shqipërisë janë:
a) Presidenti i Republikës;
b) Kryeministri.
2. Titullarët e institucioneve të tjera e marrin këtë të drejtë me autorizim nga Kryeministri.

6. Sa kohë mund të qëndrojë një informacion i klasifikuar dhe kush vendos për afatin e ruajtjes së tij?

1. Informacioni klasifikohet për aq kohë sa e kërkon interesi i sigurisë kombëtare.
2. Autoriteti klasifikues cakton afatin e ruajtjes së klasifikimit të informacionit sipas vlerave të tij.
3. Një autoritet klasifikues mund ta zgjasë kohëzgjatjen e klasifikimit ose të riklasifikojë një informacion për periudha të vazhdueshme, që nuk i kalojnë 10 (dhjetë) vjet, në përputhje me dispozitat e këtij ligji.

4. Rregullat për klasifikimin “sekret shtetëror” të informacionit përcaktohen në rregulloren, që miratohet me vendim të Këshillit të Ministrave.

7. Cilat janë elementet që duhet të përmbajë një informacion për t’u identifikuar si sekret shtetëror?

Çdo sekret shtetëror në procesin e klasifikimit duhet të përmbajë:
a) njërin nga katër nivelet e klasifikimit;
b) identitetin dhe pozitën e autoritetit klasifikues;
c) institucionin apo zyrën e origjinës;
ç) udhëzimet e deklasifikimit, nëse përcaktohen të tilla nga autoriteti klasifikues.

8. Si organizohet dhe funksionon njësia përgjegjëse për informacionin e klasifikuar në një institucion shtetëror?

1. Njësia organizative përgjegjëse për informacionin e klasifikuar përgjigjet për marrjen, dërgimin, regjistrimin, shpërndarjen, shumëfishimin, ruajtjen dhe arkivimin e informacionit të klasifikuar.
2. Funksionet e njësisë organizative përgjegjëse për informacionin e klasifikuar, me qëllim administrimin e tij, kryhen nga struktura/strukturat përgjegjëse për protokoll-arkivin, kartotekën në institucionet e administratës publike që administrojnë informacion të klasifikuar.
3. Njësia organizative përgjegjëse për informacionin e klasifikuar organizohet dhe vendoset në mjedise të përshtatshme në përputhje me masat që sigurojnë mbrojtjen e informacionit të klasifikuar, duke zbatuar standardet e sigurisë.
4. Rregullat e detajuara për funksionimin e njësisë organizative përgjegjëse për informacionin e klasifikuar dhe punën me informacionin e klasifikuar përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

9. Cilat janë rregullat për regjistrimin dhe shfrytëzimin e informacionit të klasifikuar?

1. Shfrytëzimi i informacionit të klasifikuar kryhet me qëllim ushtrimin e një detyre, në bazë të parimit “nevojë për njohje”, me miratim të titullarit të institucionit përkatës dhe vetëm nga persona të certifikuar përshtatshmërisht.
2. Shumëfishimi i informacionit të klasifikuar kryhet vetëm në njësitë organizative përgjegjëse për informacionin e klasifikuar, pas miratimit të titullarit të institucionit.
3. Përkthimi, riprodhimi, fragmentarizimi i një dokumenti ose i një materiali të klasifikuar, ruan klasifikimin e dokumentit origjinal dhe përmban të gjitha shenjëzimet e informacionit të klasifikuar.
4. Në rastet e sekuestrimit të informacionit të klasifikuar nga organi procedues, në përputhje me dispozitat e Kodit të Procedurës Penale, organi procedues zbaton dispozitat e këtij ligji për regjistrimin, shfrytëzimin, administrimin dhe ruajtjen e informacionit të klasifikuar.
5. Rregullat për regjistrimin, shfrytëzimin, shumëfishimin, riprodhimin dhe përkthimin e informacionit të klasifikuar “sekret shtetëror” përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

10. Cilat janë rastet kur informacioni i klasifikuar nuk mund të deklasifikohet sipas Ligjit nr. 10/2023?

Përveç kur parashikohet ndryshe në këtë ligj, një informacion mund të përjashtohet nga deklasifikimi kur ekspozimi i tij:
a) zbulon identitetin e burimit konfidencial, zbatimin e një metode apo të një burimi informativ;
b) nxjerr informacion që dobëson veprimtarinë e kriptologjisë;

c) nxjerr informacion që mund të dobësojë planet e ngutshme të sigurisë kombëtare;
ç) dëmton një traktat apo marrëveshje ndërkombëtare, marrëdhëniet midis Republikës së Shqipërisë dhe shteteve të huaja/organizatave ndërkombëtare apo veprimtarinë e mëtejshme diplomatike.

11. Çfarë është procesi i zhvlerësimit të informacionit të klasifikuar dhe kur aplikohet ai?

"Zhvlerësim" është procesi i ndryshimit të autorizuar të nivelit të klasifikimit të një informacioni të klasifikuar "sekret shtetëror", që, për shkak të humbjes së disa vlerave fillestare të tij, i caktohet një nivel më i ulët klasifikimi dhe afat i ri i ruajtjes së klasifikimit.
1. Kur informacioni i klasifikuar humbet disa vlera fillestare, ai mund të zhvlerësohet duke u klasifikuar e ruajtur në një nivel më të ulët.
2. Rregullat për zhvlerësimin e informacionit të klasifikuar "sekret shtetëror" përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

II. SIGURIA E PERSONELIT

1. Çfarë kuptohet me sigurinë e personelit sipas Ligjit nr. 10/2023 dhe cilat janë qëllimet e saj?

1. Siguria e personelit është tërësia e masave dhe procedurave, mbi bazën e të cilave vlerësohet nëse një individ, duke iu referuar besnikërisë, besueshmërisë dhe sigurisë së tij, mund të autorizohet për të pasur qasje tek informacioni i klasifikuar, pa e rrezikuar sigurinë e këtij informacioni.
2. Lëshimi, refuzimi, pezullimi i përkohshëm ose heqja e "Certifikatës së sigurisë së personelit" bëhet nga AKSIK.
3. Kur ekspozohet informacioni i klasifikuar apo për shkak të një kushti, të përcaktuar nga qeveria e një shteti tjetër, arsyet e refuzimit, pezullimit të përkohshëm apo heqjes së CSP-së nuk i bëhen me dije individit, institucionit kërkues apo operatorit ekonomik.
4. Procesi i verifikimit të sigurisë vijon edhe pas pajisjes së aplikantit me CSP. Kjo përfshin vlerësim të vazhdueshëm sigurie për çdo ndryshim në sjelljen e individit, që e bën atë të cenueshëm nga pikëpamja e besnikërisë, besueshmërisë dhe e sigurisë së tij.
5. Rregullat e detajuara për sigurinë e personelit përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

2. Çfarë është "Certifikata e Sigurisë së Personelit" (CSP) ?

"Certifikata e sigurisë së personelit (CSP)" është dokumenti zyrtar i autoritetit shqiptar përgjegjës për sigurinë e informacionit të klasifikuar ose i një autoriteti kompetent përgjegjës i sigurisë së një vendi tjetër, i cili vërteton nga pikëpamja e sigurisë se një individ i plotëson kushtet e përcaktuara për njohjen, ruajtjen, administrimin dhe transferimin e informacionit të klasifikuar.

3. Cilat janë kriteret për njohjen me informacionin e klasifikuar?

1. Kanë të drejtë të njihen, të ruajnë, të administrojnë e të transferojnë informacion të klasifikuar vetëm personat, që:
a) sigurojnë të drejtën e njohjes për shkak të detyrës që kryejnë nga titullari i ministrisë/institucionit ose oficeri i sigurimit industrial i kontraktorit;
b) janë të brifuar më parë për njohjen e procedurave të sigurisë së informacionit të klasifikuar dhe të përgjegjësive individuale për shkeljet e sigurisë; dhe
c) janë të pajisur me CSP, me përjashtim të rasteve për njohjen me informacionin e klasifikuar në nivelin "I kufizuar".

2. Presidenti i Republikës së Shqipërisë, Kryeministri dhe Kryetari i Kuvendit janë të autorizuar që të kenë qasje tek informacioni i klasifikuar për shkak të kryerjes së detyrave të tyre zyrtare e pajisen me CSP pa iu nënshtruar procedurave të verifikimit të sigurisë.

4. Cilat janë mënyrat e paraqitjes së kërkesës për t'u pajisur me CSP?

1. Çdo individ, që ka zotësi të plotë për të vepruar dhe është në kushtet e zbatimit të parimit "nevojë për njohje", mund të pajiset me CSP të vlefshme, kur kërkesa dhe dokumentacioni përkatës i adresohet AKSIK-ut nëpërmjet mënyrave, si më poshtë vijon:
a) Me kërkesë të titullarëve të ministrive dhe të institucioneve shtetërore për punonjësit, stafet e tyre dhe individë të tjerë, të kontraktuarit ose kategoritë e individëve të parashikuar për të marrë pjesë në një prokurim në fushën e mbrojtjes e të sigurisë, që përmban informacion të klasifikuar;
b) Me kërkesë të autoritetit homolog të një vendi tjetër, anëtar i NATO-s, i Bashkimit Evropian ose i vendit me të cilin Republika e Shqipërisë ka nënshkruar dhe është në fuqi marrëveshja e përbashkët për mbrojtjen e informacionit të klasifikuar;
c) Me kërkesë të autoritetit kompetent të sigurisë së NATO-s, të një strukture të saj apo të Bashkimit Evropian;
ç) Me kërkesë të drejtpërdrejtë të administratorit të një operatori ekonomik vendas, në kuadrin e procedurave për pajisje me CSI e CSP, sipas kërkesave të legjislacionit në fuqi.

5. Cilat janë tipet e CSP që lëshohen nga AKSIK:

1. AKSIK-u lëshon CSP për njohjen, ruajtjen, administrimin apo transferimin e informacionit të klasifikuar:
a) të prodhuar nga institucionet tona shtetërore ose/dhe të përftuara në kuadrin e bashkëpunimit dy-ose shumëpalësh me shtete dhe organizata të tjera ndërkombëtare;
b) të NATO-s;
c) të Bashkimit Evropian.
2. Modelet për tipat e CSP-së miratohen nga AKSIK-u.
3. CSP për njohjen, ruajtjen, administrimin apo transferimin e informacioneve të klasifikuara të NATO-s dhe të Bashkimit Evropian lëshohen në gjuhën angleze dhe në përputhje me standardet e kërkesat e këtyre organizatave.

6. Cilët janë nivelet e CSP-së që lëshohet nga AKSIK-u

1. Nivelet e CSP-së që lëshohen nga AKSIK-u janë:
a) "konfidencial";
b) "sekret";
c) "tepër sekret".
2. Njohja me informacionin e klasifikuar kryhet në përputhje me nivelin e CSP-së. Zotëruesi i një CSP-je me nivel më të lartë ka të drejtë që, në kushtet e nevojës për njohje, të ketë akses tek informacione të klasifikuara të një kategorie më të ulët.
3. AKSIK-u lëshon CSP në nivel më të ulët se ai që është kërkuar, në rastet kur:
a) konstatohet se një individ nuk është në kushtet e nevojës për njohje të informacionit të klasifikuar në nivelin e kërkuar;
b) diktohet nga rezultatet e përftuara nga vlerësimi i sigurisë.

7. Cilat janë afatet e lëshimit të CSP ?

Afati i përgjithshëm për kryerjen e procedurave të verifikimit fillon vetëm pas paraqitjes së plotë dhe pranimit të dokumentacionit nga ana e AKSIK dhe zgjat deri në 120 ditë kalendarike.

Ky afat mund të jetë më i gjatë kur verifikimet kushtëzohen nga kryerja e procedurave në bashkëpunim me autoritetet e sigurisë kombëtare të vendeve të tjera, ose kur drejtori i AKSIK udhëzon kryerjen e verifikimeve shtesë.

8. Sa është afati i vlefshmërisë së një CSP ?

CSP e lëshuar nga niveli "konfidencial" e më lart ka një afat vlefshmërie deri në 5 (pesë) vjet.

9. Çfarë kuptojmë me "Verifikim të Sigurisë" ?

"Verifikimi i sigurisë", është tërësia e masave dhe e procedurave të aplikuara ndaj një individi, mbi bazën e të cilave do të vlerësohet lëshimi, refuzimi, pezullimi i përkohshëm, ndërprerja e procedurave ose heqja e "Certifikatës së sigurisë së personelit".

10. Cili është rrethi i personave që verifikohen?

1. Verifikimi i sigurisë përfshin:

a) vetëm personin kërkues dhe lidhjet influencuese me interes, kur kërkohet njohja me informacionin e klasifikuar, të nivelit "konfidencial";

b) personin kërkues, fëmijët, bashkëshortin/bashkëshorten, bashkëjetuesin/bashkëjetuesen dhe lidhjet influencuese me interes, kur kërkohet njohja me informacionin e klasifikuar, të nivelit "sekret";

c) personin kërkues, fëmijët, bashkëshortin/bashkëshorten, bashkëjetuesin/bashkëjetuesen, prindërit, lidhjet influencuese me interes dhe personat e tjerë, që jetojnë së bashku në të njëjtën familje, kur kërkohet njohja me informacionin e klasifikuar, të nivelit "tepër sekret".

2. Verifikimi i sigurisë i lidhjeve të ngushta familjare dhe atyre influencuese me interes, të përcaktuara në shkronjat: "a", "b" e "c", të pikës 1, të këtij neni, kryhet për të arritur në përfundimin nëse ekziston rreziku real që kërkuesi të shantazhohet përmes këtyre lidhjeve, të cilat, në bazë të verifikimit të sigurisë, rezultojnë të përfshira në veprimtari:

a) spiunazhi;

b) terrorizmi;

c) krimi të organizuar.

11. Si duhet vepruar kur një punonjës i pajisur me CSP transferohet në një institucion tjetër, në një pozicion pune që kërkohet CSP e vlefshme?

Në rastet kur një individ, i cili zotëron një CSP të vlefshme, transferohet në një pozicion pune që, sipas listës së funksioneve organike të miratuar të institucionit të ri duhet të ketë CSP, atëherë AKSIK-u, pas kërkesës së arsyetuar me shkrim të institucionit të ri, bën konfirmimin e vlefshmërisë së CSP-së dhe modelimin e saj, në përputhje me të dhënat e reja të pozicionit të punës.

12. Cilat janë rastet e refuzimit, heqjes dhe pezullimit të përkohshëm të CSP-së

AKSIK-u ka të drejtë të marrë vendim për refuzimin, heqjen ose pezullimin e përkohshëm të CSP-së, në rastet kur nëpërmjet autoriteteve verifikuese ose/dhe strukturave shtetërore të përfshira në procesin e verifikimit është përftuar informacion, sipas të cilit vlerësohet se pajisja ose mbajtja e mëtejshme e CSP-së nga një individ i caktuar përbën rrezik të papranueshëm sigurie, referuar kritereve të parashikuara në nenin 12, të VKM së sipërcituar.

13. Sa është kohëzgjatja e pezullimit?

1. Vendimi për pezullimin e përkohshëm të CSP-së është i vlefshëm deri në momentin e shuarjes së rrethanave, që përbëjnë rrezik të papranueshëm sigurie ose deri në momentin kur CSP-së i ka përfunduar afati i vlefshmërisë.
2. Gjatë kohëzgjatjes së pezullimit të CSP-së, titullari i institucionit shtetëror dhe, sipas rastit, administratori i operatorit ekonomik kanë detyrim të marrin masat përkatëse për ndalimin e aksesit tek informacioni i klasifikuar për individin, të cilit i është pezulluar CSP-ja.

14. Sa është afati i riparaqitjes së kërkesës në rastet e refuzimit apo të heqjes së CSP-së?

1. Individët, të cilëve u është refuzuar ose hequr CSP-ja, kanë të drejtë të paraqesin kërkesë përsëri, me kusht që të ketë kaluar një vit kalendarik nga data e shkresës njoftuese për heqjen ose refuzimin e CSP-së, adresuar titullarit të institucionit, ku bën pjesë kërkuesi.
2. Pas riparaqitjes së kërkesës, referuar rasteve të pikës 1, të këtij neni, ndiqen procedurat e verifikimit të sigurisë, në përputhje me kriteret e parashikuara në këtë rregullore.

15. Si është e rregulluar e drejta e ankimit për rastet kur një individi i refuzohet, hiqet apo pezullohet CSP?

Njoftimi për vendimin e marrë nga AKSIK-u për refuzim, heqje ose pezullim të përkohshëm të CSP-së i komunikohet me shkrim titullarit të strukturës kërkuese, i cili ka të drejtë të paraqesë kërkesë me shkrim për rishqyrtimin e vendimit të marrë nga AKSIK-u.
Kjo kërkesë i adresohet titullarit të AKSIK-ut brenda 15 (pesëmbëdhjetë) ditëve kalendarike nga data e marrjes së njoftimit të vendimit për refuzimin, heqjen ose pezullimin e përkohshëm të CSP-së.
Titullari i AKSIK-ut e shqyrton kërkesën e paraqitur brenda 30 (tridhjetë) ditëve kalendarike nga dita e pranimit të saj dhe njofton titullarin e strukturës kërkuese.
Në rastet e mospajtimit me përgjigjen e titullarit të AKSIK-ut, brenda 15 (pesëmbëdhjetë) ditëve kalendarike nga data e marrjes së njoftimit, titullari i strukturës kërkuese ka të drejtë të paraqesë ankim me shkrim te Kryeministri.
Kryeministri, pas marrjes së ankimit, brenda 30 (tridhjetë) ditëve kalendarike, shprehet me akt të veçantë, i cili është përfundimtar dhe i detyrueshëm për zbatim nga AKSIK-u dhe struktura që ka bërë ankimin.

16. Ripajisja me CSP

1. Ripajisja me CSP kryhet nga AKSIK-u, sipas procedurave të miratuara në këtë rregullore.
2. Procedura për ripajisjen me CSP fillon rishtazi me paraqitjen e kërkesës nga e para.
3. Kërkesa për ripajisje me CSP paraqitet në AKSIK-u jo më vonë se 150 (njëqind e pesëdhjetë) ditë kalendarike përpara përfundimit të afatit të vlefshmërisë së CSP-së ekzistuese.
4. Pas kryerjes së procedurave të riverifikimit dhe kur nuk ekzistojnë rrethana që përbëjnë pengesa ligjore, AKSIK-u bën ripajisjen e kërkuesit me CSP, sipas kritereve të parashikuara në këtë rregullore.

17. Si duhet të veprojë një individ i pajisur me CSP pasi ndërpret marrëdhëniet e punës, apo transferohet në një pozicion që nuk kërkohet mbajtja e CSP ?

Individët e pajisur me CSP në rastet e ndërprerjes së marrëdhënieve të punës apo të ndryshimit të funksionit organik, kur nuk kërkohet mbajtja e mëtejshme e CSP e dorëzojnë atë tek oficeri i sigurisë ose struktura përgjegjëse e institucionit ku ato punojnë dhe u nënshtrohen procedurave të debrifimit duke nënshkruar në dokumentin përkatës.

Ata janë përgjegjës për ruajtjen e informacionit të klasifikuar edhe pas ndërprerjes së marrëdhënieve të punës, transferimeve apo përfundimit të kontratës apo programit/projektit, që përmban informacion të klasifikuar.
Institucionet ruajnë dhe administrojnë regjistrimet (rekordet) e individëve të brifuar dhe të debrifuar.

18. Si duhet të veproj një individ për t'u pajisur me CSP kur i kërkohet për shkak të aplikimit për punë në një kompani të huaj apo organizatë ndërkombëtare ?

Në të tilla raste pajisja me CSP realizohet vetëm pas kërkesës zyrtare që i adresohet AKSIK nga Autoriteti i Sigurisë Kombëtare (NSA) i shtetit të huaj, (duhet të jetë vend anëtar i NATO-s, BE-së, ose vend me të cilin Republika e Shqipërisë ka nënshkruar marrëveshje të përbashkët për mbrojtjen e informacionit të klasifikuar), apo përmes autoritetit kompetent të sigurisë së NATO-s, të një strukture të saj, apo të BE-së.
Aplikanti plotëson dokumentacionin e kërkuar dhe vihet në kontakt me AKSIK.
AKSIK kryen procedurat e verifikimit të sigurisë dhe në përfundim, nëse konkludon për lëshimin e CSP, i adreson përgjigjen strukturës që ka paraqitur kërkesën.

19. Cili është roli i Oficerit apo Strukturës së sigurisë?

"Oficeri i sigurisë/struktura e sigurisë", punonjësi përgjegjës ose njësia strukturore e ngarkuar nga titullari i institucionit shtetëror apo operatorit ekonomik të interesuar për mbikëqyrjen dhe zbatimin e kërkesave për sigurinë e personelit dhe të disiplinave të tjera të informacionit të klasifikuar.

20. Çfarë kuptojmë me Brifim dhe Debrifim të sigurisë?

"Brifimi/debrifimi i sigurisë", tërësi instruksionesh dhe udhëzimesh sigurie, lidhur me procedurat e sigurisë së informacionit të klasifikuar dhe përgjegjësitë individuale për shkeljet e rregullave të sigurisë, të cilave u nënshtrohen individët, që, për shkak të detyrës, kanë apo mund të kenë qasje në informacionin e klasifikuar.

III. SIGURIA FIZIKE

1. Çfarë kuptojmë me siguri fizike?

Siguria fizike është tërësia e masave fizike, teknike, elektronike dhe procedurale për ruajtjen e zonave, ndërtesave, zyrave, dhomave dhe pajisjeve ku prodhohet, administrohet dhe shkatërrohet informacioni i klasifikuar.
Masat e sigurisë fizike shërbejnë për të siguruar një nivel proporcional të mbrojtjes fizike të informacionit të klasifikuar ndaj rrezikut të vlerësuar, në bazë të procesit të "Vlerësimit të rrezikut dhe kërcënimit të sigurisë".

2. Çfarë janë zonat e sigurisë?

Zonat e sigurisë janë hapësirat ku prodhohet, regjistrohet, shfrytëzohet, transmetohet, ruhet, arkivohet dhe shkatërrohet informacion i klasifikuar.
Titullari i institucionit miraton me urdhër ndarjen e zonave të sigurisë, planin dhe skemën e sigurisë fizike të objektit ku mbahet dhe administrohet informacioni i klasifikuar.
Zonat e sigurisë ndahen në tri kategori:
a) zona e sigurisë e klasit të parë;
b) zona e sigurisë e klasit të dytë;
c) zona administrative.

Informacioni i klasifikuar “sekret shtetëror” i nivelit “tepër sekret” prodhohet dhe administrohet në zonat e sigurisë së klasit të parë.
Informacioni i klasifikuar “sekret shtetëror” i nivelit “konfidencial” e lart prodhohet dhe administrohet në zonat e sigurisë së klasit të parë dhe të dytë.
Informacioni i klasifikuar “sekret shtetëror” i nivelit “i kufizuar” prodhohet dhe administrohet në zonën administrative.

3. Cila konsiderohet zonë teknikisht e sigurt?

Zonë teknikisht e sigurt është zona në të cilën organizohen takime të klasifikuara dhe kërkon mbrojtje kundër sulmeve teknike dhe përgjimeve. Zona teknikisht e sigurt u nënshtrohet kontrolleve të rregullta fizike, teknike dhe hyrja në to duhet të ketë kontroll të rreptë.
Këto zona krijohen vetëm në institucione të veçanta, si dhe gjatë zhvillimit të takimeve në funksion të aktiviteteve të NATO-s/BE-së, në të cilat trajtohet informacion i klasifikuar.
Zonat teknikisht të sigurta përcaktohen me urdhër të titullarit të institucionit, në bazë të kritereve të përcaktuara me vendim të Këshillit të Ministrave.

4. Cilat janë disa nga masat për mbrojtjen fizike të IK?

1. Informacioni i klasifikuar “sekret shtetëror” i nivelit “Tepër sekret” i NATO-s “Cosmic Top Secret (CTS)” dhe i BE-së “EU Top Secret/Tres Secret UE” prodhohet e administrohet në zonat e sigurisë të klasit të parë.
2. Informacioni i klasifikuar i nivelit “Sekret” e poshtë, për “Sekretin shtetëror”, i NATO-s dhe BE-së, prodhohet e administrohet në zonat e sigurisë të klasit të parë dhe të dytë.
3. Informacioni i klasifikuar “sekret shtetëror” i nivelit “I kufizuar”, i NATO-s “NATO Restricted (NR)” dhe i BE-së “EU Restricted/Restreint UE” mund të prodhohet dhe administrohet edhe në zonën administrative.
4. Në planin e masave, që shoqëron urdhrin për ndarjen e zonave të sigurisë, përcaktohen edhe:
a) masat e jashtme të sigurisë fizike, që duhet të përcaktojnë qartë perimetrin e sigurisë (gardhi rrethues), barrierat fizike, ndriçimin e sigurisë, mbulimi me kamera sigurie, të cilat pengojnë hyrjen e paautorizuar në zonat e sigurisë;
b) kontrolli në pikat e hyrjes, sistemin e kontrollit të brendshëm të lëvizjes dhe të zjarrit, mbikëqyrjen me kamera, skemën e vendosjes së rojeve të sigurisë;
c) masat e sigurisë fizike, që lidhen me dyert, dritaret dhe kasafortat/dollapët metalikë, të cilët duhet të pengojnë aksesin e paautorizuar dhe mundësinë e reagimit nga forcat e sigurisë.

IV. SIGURIA NË SISTEMET E KOMUNIKIMIT DHE INFORMACIONIT

1. Cili është kuptimi i sigurisë në sistemet e komunikimit dhe informacionit?

Siguria e sistemeve të komunikimit dhe informacionit është aplikimi i masave të sigurisë për mbrojtjen e sistemeve të komunikimit dhe të informacionit, në vijim, referuar si SKI, ku prodhohet, ruhet, përpunohet ose transmetohet informacioni i klasifikuar në përmbushje të objektivave të sigurisë, konfidencialitetit, integritetit, disponueshmërisë, autenticitetit dhe pamohueshmërisë.

"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.

2. Çfarë kuptojmë me akreditim të sigurisë së Sistemeve të Komunikimit të Informacionit?

Informacioni i klasifikuar prodhohet, ruhet, transmetohet vetëm në sisteme të akredituara përshtatshmërisht.
Akreditimi i sigurisë përcakton nivelin e përshtatshëm të mbrojtjes, identifikon dhe pranon riskun e mbetur, i cili duhet të monitorohet përgjatë jetëgjatësisë së sistemit.

3. Kush e bën lëshimin, refuzimin, heqjen dhe pezullimin e përkohshëm të Deklaratës së Akreditimit të Sigurisë?

Lëshimi, refuzimi, pezullimi i përkohshëm ose heqja e Deklaratës së Akreditimit të Sigurisë (DAS) bëhet nga AKSIK-u.
Njoftimi për vendimin e marrë nga AKSIK-u për refuzimin, heqjen ose pezullimin e përkohshëm të DAS-it i komunikohet me shkrim titullarit të institucionit përkatës, që ka iniciuar kërkesën për akreditimin e sigurisë së sistemit.

4. Siguria e informacionit në SKI.

Pajisjet kompjuterike dhe SKI të akredituara identifikohen, ruhen dhe mbrohen përshtatshmërisht në përputhje me nivelin më të lartë të klasifikimit të informacionit që trajtohet në to.
Informacioni i klasifikuar, që trajtohet në pajisje kompjuterike dhe SKI-në e akredituar nga AKSIK-u, asgjësohet në përputhje me procedurat e miratuara nga AKSIK-u.

5. Kërkesat e sigurisë së SKI-së

Institucionet e administratës publike dhe operatorët ekonomikë/kontraktorët, që për nevoja pune prodhojnë, ruajnë, përpunojnë, shpërndajnë ose transmetojnë informacion të klasifikuar "sekret shtetëror" të NATO-s, BE-së, shteteve dhe organizatave të huaja, me të cilat Republika e Shqipërisë ka marrëveshje sigurie nëpërmjet sistemeve të komunikimit dhe informacionit, duhet t'u përmbahen kërkesave përkatëse të sigurisë.

6. Çfarë janë masat e sigurisë së SKI-së?

Masat e sigurisë janë mekanizmat dhe procedurat e aplikuara nga subjektet, objekt i këtij ligji, me qëllim për të siguruar mbrojtjen e informacionit të klasifikuar.

7. Kush janë autoritetet e sigurisë së SKI-së?

Menaxhimi dhe garantimi i aspekteve të sigurisë së SKI-së kryhet nga autoritetet e mëposhtme të sigurisë:
1. Autoriteti Kombëtar i Sigurisë së Informacionit të Klasifikuar, i cili funksionon edhe si:
a) Autoritet Kombëtar i Akreditimit të Sigurisë (AKAS), përgjegjës për akreditimin e sigurisë të SKI-së, të cilat nuk janë pjesë e infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe sistemeve të NATO-s, BE-së dhe shteteve/organizatave të huaja që operojnë në institucionet e administratës publike;

b) Autoriteti Kombëtar i Testimit dhe Vlerësimit të Sigurisë (AKTVS), përgjegjës për testimin dhe vlerësimin e elementeve hardëare, firmëare dhe softëare të SKI-së, që përpunojnë informacion të klasifikuar, për të cilët kërkohet testim dhe vlerësim i sigurisë.
Në rast të cenimit të integritetit të informacionit të klasifikuar, në SKI subjektet, objekt i këtij ligji, informojnë në mënyrë të menjëhershme AKSIK-un.
2. Drejtoria e Shifrës, e cila funksionon edhe si:
a) Autoritet Kombëtar i Sigurisë së Komunikimeve (AKSK), përgjegjës për:
i. kontrollin e informacionit teknik kriptografik, që lidhet me mbrojtjen e informacionit të klasifikuar;
ii. garantimin e përzgjedhjes, operimit dhe mirëmbajtjes së përshtatshme të sistemeve, produkteve dhe mekanizmave kriptografikë;
iii. garantimin e përzgjedhjes, operimit dhe mirëmbajtjes së përshtatshme të pajisjeve të sigurisë së SKI-së;
iv. trajtimin e çështjeve teknike dhe të sigurisë kriptografike për aspektet e sigurisë së komunikimeve.
b) Autoritet Kombëtar i Shpërndarjes Kriptografike (AKSHK), përgjegjës për menaxhimin e materialit kriptografik dhe garantimin e ndjekjes së procedurave për mbajtjen në llogari, ruajtjen, shpërndarjen dhe shkatërrimin e materialit kriptografik kombëtar, të NATO-s, BE-së dhe shteteve ose organizatave të huaja;
c) Autoritet Kombëtar TEMPEST (AKT), përgjegjës për kontrollin dhe vlerësimin e sigurisë së emetimeve elektromagnetike të sistemeve.
3. Rregullat dhe procedurat e detajuara për sigurinë e informacionit të klasifikuar në sistemet e komunikimit dhe informacionit, përcaktohen në rregulloren e miratuar me vendim të Këshillit të Ministrave.

V. PROJEKTE TË KLASIFIKUARA DHE SIGURIA INDUSTRIALE

1. Çfarë kuptojmë me sigurinë industriale?

1. Siguria industriale është aplikimi i sistemit të masave të sigurisë, procedurave dhe rregullave bazë, përmes të cilave realizohet parandalimi i përhapjes së paautorizuar, humbjes apo shkeljes së sigurisë së informacionit të klasifikuar, i cili trajtohet në kushtet e zbatimit të një projekti, programi, kontrate dhe nënkontrate në fushën e mbrojtjes dhe të sigurisë që përmban informacion të klasifikuar.
2. Rregullat për mbrojtjen e informacionit të klasifikuar në fushën industriale përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

2. Kush mund të iniciojë procedurat e sigurisë?

1. Institucionet e administratës publike, të cilat gjatë veprimtarisë së tyre prodhojnë, administrojnë dhe qarkullojnë informacion të klasifikuar, kanë të drejtë të iniciojnë procedurat për kryerjen e një prokurimi në fushën e mbrojtjes dhe të sigurisë që përmban informacion të klasifikuar, sipas parashikimeve të legjislacionit të posaçëm të prokurimit në këtë fushë.
2. Çdo institucion i administratës publike, në cilësinë e autoritetit kontraktor, ka përgjegjësi që gjatë hartimit të dokumentacionit të tenderit apo zbatimit të kontratës në fushën e mbrojtjes dhe të sigurisë, që përmban informacion të klasifikuar, të aplikojë sistemin e masave të sigurisë që garanton mbrojtjen e këtij informacioni, sipas kërkesave të përcaktuara në të gjitha disiplinat e sigurisë së informacionit të klasifikuar.
3. Operatorët ekonomikë të interesuar për të marrë pjesë në një prokurim në fushën e mbrojtjes dhe të sigurisë, i cili përmban informacion të klasifikuar, u nënshtrohen rregullave specifike të sigurisë.

4. Angazhimi i operatorëve ekonomikë në një prokurim në fushën e mbrojtjes dhe të sigurisë, që përmban informacion të klasifikuar në nivelin "Konfidencial" e lart, bëhet vetëm pasi më parë operatori ekonomik është i pajisur me nivelin e kërkuar të Certifikatës së Sigurisë Industriale (CSI).

3. Çfarë është "Certifikata e Sigurisë Industriale" (CSI)?

"Certifikata e sigurisë industriale (CSI)" është dokumenti zyrtar i autoritetit shqiptar përgjegjës për sigurinë e informacionit të klasifikuar ose i një autoriteti kompetent përgjegjës i sigurisë së një vendi tjetër, i cili vërteton nga pikëpamja e sigurisë se një operator ekonomik ka kapacitetet dhe aftësitë organizative, teknike e fizike dhe i plotëson standardet e përcaktuara për njohjen, ruajtjen dhe administrimin e informacionit të klasifikuar në një projekt/program apo kontratë/nënkontratë, që përmban informacion të klasifikuar.

4. Cilat janë mënyrat e aplikimit për t'u pajisur me CSI?

1. Aplikimi për pajisje me CSI i adresohet AKSIK-ut.

2. Mënyrat e aplikimit për t'u pajisur me CSI janë:
a) me kërkesë të autoritetit kontraktor;
b) me kërkesë të autoritetit kompetent, përgjegjës për sigurinë e informacionit të klasifikuar të një vendi anëtar të NATO-s, BE-së ose të një vendi, me të cilin është nënshkruar dhe ka hyrë në fuqi marrëveshja e sigurisë;
c) me kërkesë të autoritetit kompetent, përgjegjës për sigurinë e informacionit të klasifikuar të NATO-s, BE-së apo të një strukture tjetër brenda këtyre dy organizatave, në cilësinë e autoritet kontraktor;
ç) me kërkesë të drejtpërdrejtë të operatorit ekonomik vendas, vetëm kur:
i. operatori ekonomik i interesuar i plotëson të gjitha kushtet paraprake të parashikuara në pikën 1, të nenit 14, të vendimit nr. 659, datë 23.10.2024 "Për miratimin e rregullores "Për sigurinë industriale, rregullat, procedurat dhe kërkesat për mbrojtjen e informacionit të klasifikuar gjatë prokurimit në fushën e mbrojtjes dhe të sigurisë";
ii. operatori ekonomik i interesuar, gjatë 5 (pesë) viteve të fundit ka qenë të paktën 1 (një) herë palë në një kontratë/nënkontratë në fushën e mbrojtjes dhe të sigurisë, e cila ka trajtuar informacion të klasifikuar, e vërtetuar me shkrim nga autoriteti kontraktor përkatës.

3. Aplikimi sipas shkronjave "a", "b" dhe "c", të pikës 2, të këtij neni, realizohet kur:
a) ekziston interesi për pjesëmarrje në një prokurim në fushën e mbrojtjes dhe të sigurisë, i cili përmban informacion të klasifikuar ose kur operatori ekonomik është në kushtet e zbatimit të kontratës/nënkontratës, që përmban informacion të klasifikuar;
b) operatori ekonomik i interesuar plotëson të gjitha kushtet paraprake të parashikuara në pikën 1, të nenit 14, të kësaj rregulloreje;
c) kërkesa për pajisje me CSI shoqërohet me dokumentacionin e apilikimit, sipas përcaktimeve të bëra në nenin 16, të kësaj rregulloreje.

5. Kushtet paraprake të aplikimit për pajisje me CSI

1. Të drejtën e aplikimit për fillimin e procedurave për pajisje me CSI të vlefshme për pjesëmarrje në një prokurim në fushën e mbrojtjes dhe të sigurisë i cili përmban informacion të klasifikuar, sipas mënyrave të parashikuara në nenin 15 të kësaj Rregulloreje, e gëzon vetëm operatori ekonomik, i cili është i regjistruar në regjistrin tregtar sipas legjislacionit shqiptar i cili ka status aktiv dhe plotëson të gjitha kushtet e mëposhtme:
a. të ketë strukturë të qartë dhe të qëndrueshme organizative;

b. të paktën gjatë tre viteve të fundit rezulton me bilance pozitive, referuar pasqyrave financiare të vërtetuara nga administrata tatimore;

c. gjatë tre viteve të fundit nuk është i përjashtuar nga e drejta për të fituar kontrata publike;

ç. gjatë tre viteve të fundit nuk është i përjashtuar nga pjesëmarrja në procedurat e prokurimit në fushën e mbrojtjes dhe të sigurisë që përmbajnë informacion të klasifikuar apo prokurimet publike.

Ky kusht konsiderohet i paplotësuar për operatorët ekonomikë që janë në proces gjyqësor për procedurë përjashtimi, deri në momentin kur gjykata kompetente të shprehet me vendim përfundimtar për çështjen në themel;

d. gjatë dhjetë viteve të fundit nuk i është refuzuar, hequr, Certifikata e Sigurisë Industriale (CSI);

dh. rezulton i pajisur me licencën/at profesionale, në lidhje me veprimtarinë për të cilën është i regjistruar, vërtetuar me dokumentacion përkatës origjinal, ose të noterizuar;

e. nuk është në likuidim, në proces falimentimi apo në pritje të procedurave të falimentimit, vërtetuar me deklaratë noteriale të administratorit të operatorit ekonomik dhe me vërtetim të lëshuar nga Gjykata;

ë. nuk rezulton në kushtet e ndalimit të ushtrimit të veprimtarisë, vërtetuar me deklaratë noteriale të administratorit të operatorit ekonomik;

f. administratori, pronari/pronarët, operatori ekonomik nuk rezultojnë të dënuar, vërtetuar me Certifikatë të Gjendjes Gjyqësore;

g. ashkëpronarët, (kur ka të tillë), nuk janë në kushtet e konfliktit të interesit lidhur me strukturën e pronësisë dhe pjesët takuese, vërtetuar me deklaratë noteriale;

gj. struktura e pronësisë e operatorit ekonomik të interesuar është në masën 51% e më lart në zotërim të individëve me shtetësi shqiptare, si dhe jo më shumë se 5% në zotërim të individëve që kanë shtetësinë e një vendi jo anëtar të NATO-s, BE-së apo të një shteti me të cilin vendi ynë nuk ka nënshkruar Marrëveshje Sigurie, konfirmuar sipas ekstraktit të QKB-së;

h. referuar vërtetimit të lëshuar nga Gjykata kompetente, rezulton se në drejtim të operatorit ekonomik nuk ekziston ndonjë procedim penal;

i. referuar vërtetimit të lëshuar nga Prokuroria, rezulton se në drejtim të operatorit ekonomik nuk është filluar ndonjë çështje penale;

j. operatori Ekonomik rezulton se i ka paguar taksat vendore, konfirmuar përmes vërtetimit të lëshuar nga Administrata Bashkiake;

k. operatori Ekonomik i cili ka kredi të marra në sistemin bankar, rezulton se i shlyen ato rregullisht, konfirmuar përmes vërtetimit të lëshuar nga Banka e Shqipërisë;

l. operatori Ekonomik i cili ka marrë hua, rezulton se i shlyen ato rregullisht, konfirmuar përmes Deklaratës së Pronarit/Administratorit/ përpara noterit.

2. Operatori ekonomik duhet të paraqesë dokumente që vërtetojnë plotësimin e kushteve të parashikuara në pikën 1, të nenit 14.

3. Konstatimi për mosplotësimin e një apo më shumë kritereve të parashikuara në pikën 1 të këtij neni, përbën shkak të mjaftueshëm për mosfillimin apo ndërprerjen e menjëhershme të procedurave për pajisje me CSI.

6. Dokumentacioni i kërkesës për pajisje me CSI

1. Dokumentacioni i kërkesës për t'u pajisur me CSI përmban:
a) kërkesën për lëshimin e CSI-së, adresuar AKSIK-ut, sipas modelit të përcaktuar e të miratuar nga ky autoritet;
b) pyetësorin e sigurisë industriale dhe autorizimin për dhënien e pëlqimit për kryerjen e verifikimeve dhe ruajtjen e "sekretit shtetëror", sipas modelit të përcaktuar e të miratuar nga AKSIK-u;
c) ekstraktin historik të regjistrit tregtar për të dhënat e subjektit, (operatorit ekonomik);
ç) dokumentin e lëshuar nga zyra e përmbarimit, që vërteton se për kapitalet/asetet e operatorit ekonomik, nuk ekziston një urdhër sekuestroje;
d) dokumentin e lëshuar nga administrata tatimore, që vërteton se operatori ekonomik i ka plotësuar detyrimet fiskale;
dh) dokumentin e lëshuar nga administrata tatimore, që vërteton se operatori ekonomik i ka paguar të gjitha detyrimet e sigurimeve shoqërore;
e) faturën bankare, që konfirmon kryerjen e pagesës së shërbimit për fillimin e procedurave për pajisjen me CSI, në shumën 300 000 (treqind mijë) lekë.
2. Kërkesa për pajisje me CSI shoqërohet me dokumentacionin e kërkuar, sipas përcaktimeve të bëra në pikën 1, të nenit 14, të kësaj rregulloreje.
3. Dokumentet e kërkesës për pajisje me CSP, sipas këtij neni, duhet të jenë origjinale, të lëshuara nga autoritetet përkatëse, brenda tre muajve të fundit. Ato i adresohen AKSIK-ut, të shoqëruara me pyetësorët e sigurisë për verifikimin e personelit që do të njihet me informacionin e klasifikuar dhe dokumentet e tjera, sipas kërkesave të legjislacionit në fuqi për sigurinë e personelit.

7. Cili është afati i vlefshmërisë së një CSI ?

CSI-ja e lëshuar nga AKSIK ka një afat vlefshmërie deri në 5 (pesë) vite kalendarike.
Ky afat është i vlefshëm për të gjitha nivelet dhe tipat e CSI-së.

8. Vlefshmëria dhe tipet e CSI.

1. CSI-ja e lëshuar nga autoriteti përgjegjës për sigurinë e informacionit të klasifikuar është e vlefshme:
a) vetëm për qasje tek informacioni i klasifikuar;
b) për qasjen, të drejtën e ruajtjes dhe të administrimit të informacionit të klasifikuar në mjediset e operatorit ekonomik;
c) për qasjen, të drejtën e ruajtjes dhe të administrimit të informacionit të klasifikuar, si dhe përdorimit të sistemeve të akredituara të komunikimit dhe të informacionit në mjediset e operatorit ekonomik.
2. CSI-ja lëshohet në nivelin "Konfidencial", "Sekret" dhe "Tepër sekret" për informacionin e klasifikuar "sekret shtetëror" të NATO-s dhe të BE-së.
3. Autoriteti kontraktor verifikon vlefshmërinë dhe tipin e CSI-së tek autoriteti përgjegjës për sigurinë e informacionit të klasifikuar, përpara se operatori ekonomik i interesuar dhe personeli i tij të kenë qasje tek informacioni i klasifikuar.

9. Në cilat raste hiqet CSI-ja?

AKSIK-u merr vendimin për heqjen e CSI-së, në rastet kur:

a) përmes strukturave shtetërore të ngarkuara me procesin e verifikimit të sigurisë, deklarimeve të OSI/zëvendësit të tij, autoriteteve kontraktore, ose inspektimeve të kryera, përfton raporte zyrtare, informacion të vërtetuar apo në kuadër të dyshimeve të arsyeshme, sipas të cilave arrihet në përfundime të arsyetuara se mbajtja e mëtejshme e CSI-së, e lëshuar për një operator ekonomik, përbën rrezik të papranueshëm për sigurinë e informacionit të klasifikuar, referuar kërkesave të përcaktuara në këtë rregullore;
b) konfirmohet se raportet në strukturën e pronësisë i përkasin 50% e më lart personave fizikë e juridikë të huaj;
c) vërtetohet ekzistenca e rrethanave të parashikuara në pikat 2 dhe 3, të nenit 21, të kësaj rregulloreje.

10. Kur pezullohet CSI-ja?

1. AKSIK-u merr vendimin për pezullimin e përkohshëm të CSI-së, kur konstatohet se:
a) operatori ekonomik është nën potencialin e mundshëm të influencës së ushtruar për llogari të interesave të huaja, deri në marrjen e masave të kufizimit të rrezikut të sigurisë;
b) janë konstatuar shkelje të rregullave të sigurisë ose mospërmbushje të detyrimeve të parashikuara në ISP;
c) janë siguruar informacione apo raporte zyrtare, sipas të cilave krijohen dyshime që duhen konfirmuar se mbajtja e mëtejshme e CSI-së, e lëshuar për një operator ekonomik, përbën rrezik të papranueshëm për sigurinë e informacionit të klasifikuar.
2. Vendimi për pezullimin e CSI-së është i vlefshëm deri në momentin e sqarimit të fakteve apo shuarjes së rrethanave, që përbëjnë rrezik të papranueshëm për sigurinë e informacionit të klasifikuar ose deri në momentin kur CSI-së i mbaron afati i vlefshmërisë së saj.