REGLUGERÐ

um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála.

I. KAFLI
Almenn ákvæði.

1. gr.
Markmið.

Markmið reglugerðar þessarar er:

a) að vernda gögn skv. 2. gr., sem mikilvægt er að óviðkomandi fái ekki aðgang að, enda hafi þau að geyma upplýsingar um öryggi ríkisins, varnarmál eða samskipti við önnur ríki eða fjölþjóðastofnanir sem mikilvægir almannahagsmunir krefjast að fari leynt,
b) að uppfylla skuldbindingar samkvæmt alþjóðasamningum á sviði öryggis- og varnarmála sem kveða á um trúnað og sérstaka varðveislu tiltekinna upplýsinga eða gagna,
c) að tryggja viðeigandi meðferð og öryggi slíkra gagna, hvaðan sem þau eru upprunnin og
d) að kveða á um öryggisvottun fyrirtækja sem hana þurfa vegna útflutningshagsmuna.

2. gr.
Gildissvið.

Reglugerð þessi gildir um:

a) trúnaðarupplýsingar, sem varnarmálalög, nr. 34/2008, taka til, þ.m.t. öryggi og meðferð þeirra,
b) öryggisvottanir og öryggisviðurkenningar fyrir einstaklinga, fyrirtæki, þ.m.t. birgja, þjónustuaðila og útflytjendur, stofnanir, upplýsingakerfi, búnað og mannvirki á sviði öryggis- og varnarmála sem varnarmálalög taka til,
c) aðgang að trúnaðarupplýsingum, öryggisvottanir og öryggisviðurkenningar á grundvelli samnings Íslands og Evrópusambandsins um öryggisverklag vegna skipta á trúnaðarflokkuðum upplýsingum frá 12. júní 2006, ásamt viðauka við hann, samkomulagi um öryggistilhögun milli utanríkisráðuneytis lýðveldisins Íslands (utanríkisráðuneytisins), öryggisdeildar aðalskrifstofu ráðs ESB (GSCSO) og öryggismálaskrifstofu framkvæmdastjórnar Evrópubandalaganna (ECSD) vegna verndar trúnaðarflokkaðra upplýsinga sem lýðveldið Ísland og ESB hafa skipti á,
d) aðgang að trúnaðarupplýsingum, öryggisvottanir og öryggisviðurkenningar á grundvelli almenns samnings um öryggi varðandi gagnkvæma vernd og miðlun trúnaðarflokkaðra upplýsinga milli Danmerkur, Finnlands, Íslands, Noregs og Svíþjóðar frá 7. maí 2012 og
e) aðgang að trúnaðarupplýsingum, öryggisvottanir og öryggisviðurkenningar á grundvelli annarra alþjóðasamninga sem Ísland er aðili að.

3. gr.
Skilgreiningar.

Merking hugtaka er sem hér segir:

a) **Aðgangsheimild** *(Authorisation for Access):* Ákvörðun tekin af forsvarsmanni stofnunar eða fyrirtækis um að einstaklingi sé heimill aðgangur að öryggissvæðum eða upplýsingum á ákveðnu trúnaðarstigi, standist hann öryggisvottun.
b) **Bakgrunnsskoðun** *(Background Check/Vetting):* Athugun öryggisstjórnvalds á því hver viðkomandi einstaklingur er og á upplýsingum lögreglu, m.a. um sakaferil hans, þ.m.t. hvort hann eigi afbrotaferil að baki, sem liður í mati á því hvort óhætt sé að gefa út öryggisvottun honum til handa og þar með heimila honum aðgang að viðkvæmum svæðum og trúnaðarupplýsingum.
c) **Birgir** *(Supplier):* Aðili sem selur vörur sem við koma meðferð trúnaðarupplýsinga og falla undir reglugerð þessa.
d) **Flutningsvottorð** *(Courier Certificate):* Staðfesting stofnunar á að sending, sem inniheldur trúnaðarupplýsingar, sé heimiluð og að einstaklingur, sem þær flytur, geri það í umboði stjórnvalda.

e) **Fyrirtæki** *(Organisation outside the Government/Company/Firm):* Lögaðili, þ.m.t. birgir, þjónustuaðili eða útflytjandi, sem kemur að meðferð trúnaðarupplýsinga sem falla undir reglugerð þessa.
f) **Innkaupastofnun** *(Procuring Entity):* Stjórnsýslustofnun sem kaupir vörur eða þjónustu frá lögaðila sem ekki fellur undir stjórnsýsluna.
g) **Rekstrarsvæði** *(Administrative Area/Zone):* Aðgangsstýrt svæði sem staðist hefur öryggisúttekt viðeigandi öryggisstjórnvalds og hlotið viðurkenningu til að meðhöndlaðar séu trúnaðarupplýsingar að trúnaðarstiginu *„takmarkaður aðgangur“* samkvæmt reglugerð þessari, sbr. 5. og 7. gr.
h) **Skjal** *(Document):* Hvers konar gagn, jafnt ritað sem í öðru formi, er hefur að geyma upplýsingar og hefur orðið til, borist eða verið viðhaldið við starfsemi á vegum stofnunar eða einstaklings.
i) **Stofnun** *(Organisation):* Stjórnsýslustofnun sem reglugerð þessi gildir um.
j) **Trúnaðarflokkaðar upplýsingar** *(Classified Information):* Trúnaðarupplýsingar sem merktar eru ákveðnu trúnaðarstigi og aðgangi að þeim er stýrt m.t.t. trúnaðarstigs, öryggisvottunar og/eða -viðurkenningar og þess hverjir þurfa á upplýsingunum að halda.
k) **Trúnaðargögn** *(Classified Data):* Það efnislega form sem geymir trúnaðarupplýsingar.
l) **Trúnaðarstig** *(Security Classification/Security Marking):* Flokkun og merking trúnaðarupplýsinga eftir því hversu alvarlegt það væri ef óviðkomandi aðilar kæmust yfir þær.
m) **Trúnaðarskjalasafn** *(Registry):* Skjalasafn trúnaðarskjala þar sem fram fer móttaka skráning, dreifing, vistun og eyðing trúnaðarupplýsinga innan viðkomandi stofnunar eða fyrirtækis.
n) **Trúnaðarupplýsingar**: Upplýsingar sem reglugerð þessi tekur til og gæta þarf sérstaks trúnaðar um.
o) **Upplýsingar** *(Information):* Hvers kyns upplýsingar óháð formi þeirra, þ.m.t. skjöl (rafræn eða á pappír), svo sem kort, ljósmyndir eða mynd- og hljóðupptökur, eða önnur gögn.
p) **Yfirmaður öryggismála** *(Security Officer):* Sá starfsmaður stofnunar eða fyrirtækis sem hefur verið falið af forstöðumanni hennar eða þess að bera ábyrgð á framkvæmd reglugerðar þessarar.
q) **Þjónustuaðili** *(Service Provider):* Aðili sem veitir þjónustu sem viðkemur meðferð trúnaðarupplýsinga samkvæmt reglugerð þessari.
r) **Öruggt upplýsingakerfi** *(Secure Network/Communication Information System (CIS)):* Skipulögð samsetning jaðarbúnaðar, hugbúnaðar, gagnakerfa og samskiptanets sem eru dulkóðuð með viðeigandi hætti og hafa fengið öryggisviðurkenningu samkvæmt reglugerð þessari.
s) **Öryggishæfi** *(Security Competence):* Hæfi einstaklings, stofnunar, fyrirtækis, svæðis eða búnaðar til að hljóta öryggisvottun og/eða -viðurkenningu fyrir ákveðið trúnaðarstig.
t) **Öryggissamningur** *(Security Agreement/Security Aspects Letter):* Samningur á milli stjórnsýslustofnunar og birgis, þjónustuaðila eða útflytjanda sem er gerður við öryggisflokkuð vöru- eða þjónustukaup eða útflutning áður en veittur er aðgangur að trúnaðarupplýsingum.
u) **Öryggisstjórnvald** *(National Security Authority):* Miðlæg stofnun sem fyrir hönd ríkisins samræmir og er eftirlitsaðili með meðferð og varðveislu trúnaðarupplýsinga, annast framkvæmd bakgrunnsskoðana og ákvörðun öryggisvottunar og/eða -viðurkenningar fyrir einstaklinga, stofnanir, fyrirtæki, svæði, upplýsingakerfi og búnað innanlands, sem og gagnvart erlendum ríkjum eða alþjóðastofnunum, sbr. einnig 1. mgr. 4. gr.
v) **Öryggissvæði** *(Secure Area/Security Zone):* Aðgangsstýrt svæði sem staðist hefur öryggisúttekt öryggisstjórnvalds og hlotið viðurkenningu til að meðhöndlaðar séu á því trúnaðarupplýsingar merktar trúnaðarstiginu *„trúnaðarmál“* og hærra samkvæmt reglugerð þessari.
w) **Öryggisúttekt** *(Inspection):* Eftirlit öryggisstjórnvalds með stofnunum, fyrirtækjum, svæðum, aðstöðu og/eða húsrými, upplýsingakerfum og búnaði sem hafa hlotið öryggisvottun og/eða -viðurkenningu og því hvernig framkvæmd reglugerðar þessarar er háttað.
x) **Öryggisvottun einstaklings** *(Personnel Security Clearance):* Staðfesting öryggisstjórnvalds, byggð á bakgrunnsskoðun vegna öryggishæfis einstaklings til aðgangs að trúnaðarupplýsingum að ákveðnu trúnaðarstigi.
y) **Öryggisvottun fyrirtækis** *(Facility Security Clearance):* Staðfesting öryggisstjórnvalds, byggð á bakgrunnsskoðunum einstaklinga (stjórnarformanna og/eða starfsmanna), og eftir atvikum

öryggisúttekt á aðstöðu fyrirtækis, á bærni þess til að starfa við atvinnugrein eða rannsóknir sem krefjast aðgangs að trúnaðarupplýsingum.

z) **Öryggisviðurkenning upplýsingakerfis og búnaðar** *(Security Approval/Accreditation of CIS):* Staðfesting öryggisstjórnvalds á því að kerfi og búnaður, sem trúnaðarupplýsingar eru vistaðar í, meðhöndlaðar í eða miðlað til og/eða frá, uppfylli öryggiskröfur þar um.

þ) **Öryggisviðurkenning aðstöðu** *(Facility Approval):* Staðfesting öryggisstjórnvalds sem byggist á öryggisúttekt um að ákveðið rými, svæði eða aðstaða innan stofnunar eða fyrirtækis standist kröfur um rekstrarsvæði, öryggissvæði I eða II til hýsingar á trúnaðarupplýsingum að ákveðnu trúnaðarstigi, sbr. 5. og 7. gr.

æ) **Öryggisflokkuð vöru- og þjónustukaup** *(Classified Procurement):* Kaup innkaupastofnunar sem eru þess eðlis að birgjar eða þjónustuaðilar þurfa aðgang að trúnaðarupplýsingum, búnaði eða hlut eða að þá þarf að öryggisvotta af öðrum orsökum.

4. gr.

Ábyrgð og eftirlit.

Ríkislögreglustjóri gegnir hlutverki öryggisstjórnvalds, eins og það er skilgreint í reglugerð þessari, sbr. reglur þeirra alþjóðastofnana sem þessi reglugerð varðar.

Forstöðumaður stofnunar eða framkvæmdastjóri fyrirtækis, sem hefur fengið öryggisvottun eða hefur öryggisvottaða starfsmenn að störfum, ber ábyrgð á framkvæmd reglugerðar þessarar innan þeirrar stofnunar eða fyrirtækis. Hann skal:

a) sjálfur undirgangast öryggisvottun samkvæmt reglugerð þessari,
b) fela tilteknum starfsmanni sínum að gangast undir öryggisvottun samkvæmt reglugerð þessari og gegna starfi yfirmanns öryggismála,
c) tryggja að þeir starfsmenn sem hjá stofnuninni eða fyrirtækinu starfa og þurfa aðgang að trúnaðarflokkuðum upplýsingum samkvæmt reglugerð þessari gangist undir öryggisvottun samkvæmt reglugerðinni,
c) tryggja að starfsreglur stofnunarinnar eða fyrirtækisins séu í samræmi við reglugerð þessa,
d) taka saman innanhússleiðbeiningar um meðferð trúnaðarflokkaðra upplýsinga og öryggismál á grundvelli reglugerðar þessarar, með nánari útfærslu eftir þörfum,
e) kynna starfsmönnum reglugerð þessa með reglubundnum hætti, starfsreglur stofnunarinnar eða fyrirtækisins, innanhússleiðbeiningar um öryggismál og nánari útfærslu þeirra og
f) tryggja rekstur trúnaðarskjalasafns innan stofnunar eða fyrirtækis þar sem við á.

Leiki grunur á broti á reglugerð þessari skal það tafarlaust tilkynnt yfirmanni öryggismála, forstöðumanni stofnunar, framkvæmdastjóra fyrirtækis og ríkislögreglustjóra. Ef brot er staðfest skal það tilkynnt yfirmanni öryggismála utanríkisráðuneytisins.

Ríkislögreglustjóri gerir öryggisúttektir á stofnunum, fyrirtækjum, svæðum, upplýsingakerfum og búnaði sem hann hefur öryggisvottað eða öryggisviðurkennt, sbr. 37. gr.

II. KAFLI

Trúnaðarflokkun, geymsla, meðferð og miðlun trúnaðarflokkaðra upplýsinga.

5. gr.

Trúnaðarflokkun.

Trúnaðarflokkaðar upplýsingar má eingöngu nota í þeim tilgangi sem ætlast er til og ber að meðhöndla þær í samræmi við trúnaðarflokkun samkvæmt þessari grein.

Trúnaðarflokkaðar upplýsingar má eingöngu afhenda einstaklingum sem þurfa, starfa sinna vegna, aðgang að þeim og hafa verið öryggisvottaðir samkvæmt reglugerð þessari í þeim tilgangi.

Trúnaðarupplýsingar skal flokka eftir trúnaðarstigi og skal auðkenna trúnaðarstigið með greinilegum hætti. Flokkun trúnaðarupplýsinga í trúnaðarstig byggir á mati á þeim skaða sem getur orðið komist þær í hendur óviðkomandi aðila. Trúnaðargögn skal flokka og merkja með einu af eftirfarandi trúnaðarstigum frá því hæsta a) til þess lægsta d):

a) ALGJÖRT LEYNDARMÁL („YDERST HEMMELIGT“, „COSMIC TOP SECRET“, „TRÈS SECRET UE“ eða samsvarandi) notist í þeim tilfellum þegar öryggi Íslands, annarra ríkja eða alþjóðastofnana, tengsl við erlend stjórnvöld eða alþjóðastofnanir eða aðrir grundvallar-

hagsmunir ríkisins geta orðið fyrir sérstaklega alvarlegum skaða, komist upplýsingarnar í hendur óviðkomandi aðila,

b) LEYNDARMÁL („HEMMELIGT“, „NATO SECRET“, „SECRET UE“ eða samsvarandi) notist í þeim tilfellum þegar öryggi Íslands, annarra ríkja eða alþjóðastofnana, tengsl við erlend stjórnvöld eða alþjóðastofnanir eða aðrir grundvallarhagsmunir ríkisins geta skaðast alvarlega, komist upplýsingarnar í hendur óviðkomandi aðila,

c) TRÚNAÐARMÁL („FORTROLIGT“, „NATO CONFIDENTIAL“, „CONFIDENTIEL UE“ eða samsvarandi) notist í þeim tilfellum þegar öryggi Íslands, annarra ríkja eða alþjóðastofnana, tengsl við erlend stjórnvöld eða alþjóðastofnanir eða aðrir grundvallarhagsmunir ríkisins geta skaðast, ef upplýsingarnar komast í hendur óviðkomandi aðila og

d) TAKMARKAÐUR AÐGANGUR („TIL TJENESTEBRUG“, „NATO RESTRICTED“, „RESTREINT UE“ eða samsvarandi) notist í þeim tilfellum þegar það getur verið andstætt hagsmunum Íslands, annarra ríkja eða alþjóðastofnana eða haft neikvæð áhrif á tengsl við erlend stjórnvöld eða alþjóðastofnanir að upplýsingarnar komist í hendur óviðkomandi aðila.

Gögn, sem eru merkt „NATO UNCLASSIFIED“, eru eign Atlantshafsbandalagsins og gilda reglur bandalagsins um birtingu þeirra.

Sá sem trúnaðargögn stafa frá skal tryggja að þau séu merkt réttu trúnaðarstigi. Ekki skal merkja trúnaðargögn hærra trúnaðarstigi en nauðsyn krefur. Gildistími trúnaðarstigs samkvæmt grein þessari skal ekki vera lengri en nauðsyn krefur. Merkja skal íslensk trúnaðargögn sem dreifa á erlendis „ISL“ og viðeigandi trúnaðarstigi (svo sem *„ISL Restricted“*), nema alþjóðasamningar kveði á um annað.

6. gr.

Meðferð trúnaðarflokkaðra upplýsinga.

Eftirfarandi gildir um meðferð trúnaðarflokkaðra upplýsinga:

a) upplýsingarnar skal vernda og varðveita á tryggan hátt,

b) ef upplýsingarnar eru notaðar í ný gögn skulu þau fá sama trúnaðarstig og upprunaskjalið,

c) ef upplýsingarnar eru afritaðar eða þýddar skal skjalið fá sama trúnaðarstig og upprunaskjalið. Í þýðingu á slíku trúnaðarskjali skal tilgreina að það innihaldi trúnaðarflokkaðar upplýsingar upprunaríkis eða -stofnunar,

d) ef upplýsinga með trúnaðarstigi *„algjört leyndarmál“* er ekki lengur þörf skal þeim komið fyrir í langtímavörslu, sbr. 13. gr., þeim eytt, sbr. 12. gr., eða skilað til upprunaríkis eða -stofnunar eftir því sem við á. Skjölum með trúnaðarstigið *„leyndarmál“* eða lægra skal eytt í samræmi við reglugerð þessa og

e) ef í neyðartilvikum er ekki hægt að vernda trúnaðarflokkaðar upplýsingar skal þeim eytt.

Ennfremur er óheimilt, nema með skriflegu samþykki þess ríkis eða stofnunar sem upplýsingarnar stafa frá, að:

a) breyta trúnaðarstigi skjals,

b) þýða, afrita eða eyða skjölum með trúnaðarstiginu *„algjört leyndarmál“,*

c) miðla trúnaðarflokkuðum upplýsingum til annarra ríkja, stofnana eða óviðkomandi aðila nema sérstök heimild sé fyrir hendi og þörf krefji og

d) flytja úr landi trúnaðarflokkaðar upplýsingar nema sérstök heimild sé fyrir hendi og þörf krefji.

7. gr.

Geymsla trúnaðarflokkaðra upplýsinga.

Geyma skal trúnaðarflokkaðar upplýsingar í öruggum hirslum, vottuðu upplýsingakerfi eða á þar til gerðum svæðum sem lúta ákveðnum umgengnisreglum og eru búin sérstökum öryggisbúnaði. Þessi svæði flokkast í:

a) öryggissvæði I,

b) öryggissvæði II og

c) rekstrarsvæði.

Öryggissvæði I og II eru svæði sem eru sérstaklega skilgreind og aðgangsstýrð. Þar skal vera þjófavarnarkerfi með rafrænum skynjurum sem eru tengdir við öryggismiðstöð. Öryggissvæði I er

vaktað allan sólarhringinn og er öðrum en öryggisvottuðum einstaklingum ekki heimill aðgangur að því nema með sérstakri heimild yfirmanns öryggismála. Heimilt er að sameina öryggissvæði I og II, mæli sérstakar ástæður með því og stofni það geymslu trúnaðarflokkaðra upplýsinga ekki í hættu.

Trúnaðarflokkaðar upplýsingar sem eru merktar sem:

a) *„algjört leyndarmál“* skulu geymdar á öryggissvæði I,
b) *„leyndarmál“* og *„trúnaðarmál“* skulu geymdar á öryggissvæði I eða II og
c) *„takmarkaður aðgangur“* skulu geymdar á öryggissvæði I eða II eða rekstrarsvæði, enda séu þær í viðurkenndum læstum hirslum eða á læstum skrifstofum á rekstrarsvæði.

Þegar einstaklingur, sem hefur trúnaðarflokkaðar upplýsingar undir höndum, yfirgefur skrifstofu eða vinnusvæði sitt, skal hann tryggja að þær séu geymdar í viðurkenndum læstum hirslum á öryggissvæðum, skv. 1. mgr., eftir trúnaðarstigi þeirra.

8. gr.

Miðlun trúnaðarflokkaðra upplýsinga.

Utanríkisráðuneytið annast miðlun trúnaðarflokkaðra upplýsinga innanlands sem berast erlendis frá á grundvelli alþjóðasamninga, nema þeir mæli fyrir um annað. Áður en slíkum trúnaðarflokkuðum upplýsingum er miðlað skal liggja fyrir öryggisvottun og/eða -viðurkenning fyrir viðkomandi:

a) einstakling, sem taka á við upplýsingunum, um að hann uppfylli skilyrði til að hafa aðgang að trúnaðarflokkuðum upplýsingum,
b) fyrirtæki eða stofnun, sem taka á við upplýsingunum, um að það eða hún hafi viðunandi aðstöðu, ef við á, til að geyma trúnaðarflokkaðar upplýsingar og aðgangsstýra þeim og
c) búnað, svo sem upplýsingakerfi, sem hýsa á upplýsingarnar eða miðla þeim, um að hann sé fullnægjandi með tilliti til upplýsingaöryggis, ef við á.

9. gr.

Öryggi, merking og flutningur trúnaðarflokkaðra upplýsinga.

Gæta skal öryggis trúnaðarflokkaðra upplýsinga allan líftíma þeirra.

Halda skal skrá um trúnaðarflokkaðar upplýsingar merktar *„trúnaðarmál“* og hærra þar sem skráð er móttaka, meðhöndlun, dreifing og eyðing þeirra, sbr. 13. gr.

Þegar trúnaðarflokkaðar upplýsingar eru fluttar á milli staða skulu þær tvípakkaðar í ógegnsæjum umbúðum eða umslögum. Innri umbúðir skal innsigla og merkja trúnaðarstigi, móttakanda og sendanda. Ytri umbúðir skulu innsiglaðar og eingöngu merktar móttakanda og sendanda. Þannig má senda trúnaðarflokkaðar upplýsingar merktar *„takmarkaður aðgangur“* með hefðbundnum pósti.

Trúnaðarflokkaðar upplýsingar, sem eru merktar *„trúnaðarmál“* og hærra skulu einungis fluttar milli staða í vörslu öryggisvottaðs einstaklings sem skal vera kunnugur þeim reglum sem um flutning trúnaðarflokkaðra upplýsinga gilda.

Þegar trúnaðarflokkaðar upplýsingar merktar *„trúnaðarmál“* og hærra eru fluttar á milli ríkja skal vottaður einstaklingur, sem þær flytur, hafa formleg flutningsvottorð til staðfestingar frá stofnun sem sendir skjölin. Í flutningsvottorði skal koma fram hvaðan og hvert sending skal flutt, ferðaáætlun sendils ásamt tilvísunarnúmeri í sendingu. Trúnaðarflokkaðar upplýsingar, sem sendar eru á milli ríkja, skulu undanþegnar tollskoðun við landamæraeftirlit, enda hafi einstaklingur, sem þær flytur, fyrrgreint flutningsvottorð frá stofnun.

10. gr.

Endurmat og gildistími trúnaðarflokkaðra upplýsinga.

Endurmeta skal trúnaðarstig trúnaðarflokkaðra upplýsinga reglulega eða á a.m.k. fimm ára fresti. Trúnaði skal að jafnaði aflétt af trúnaðarskjölum merktum *„algert leyndarmál“* eftir 30 ár, *„leyndarmál“* eftir 15 ár og *„trúnaðarmál“* eftir 5 ár.

11. gr.

Tölvuöryggi.

Óheimilt er að setja trúnaðarflokkaðar upplýsingar, sem falla undir gildissvið reglugerðar þessarar, á rafrænt form eða flytja þær með rafrænum hætti nema í viðurkenndu upplýsingakerfi, sbr. 22. gr. Ekki má senda framangreindar trúnaðarflokkaðar upplýsingar með almennum tölvupósti.

Öryggisvottaðir einstaklingar skulu hafa aðgang að tölvu, sem geymir trúnaðarflokkaðar upplýsingar, lokaðan í fjarveru sinni. Þeim er óheimilt að gefa öðrum upp aðgangs- og/eða lykilorð sín.

Stofnun eða fyrirtæki, sem býr yfir öryggisviðurkenndu upplýsingakerfi, skal setja reglur um aðgangsstýringu að trúnaðarflokkuðum upplýsingum, sem þar eru geymdar, til að tryggja að þeir sem hafa aðgang að upplýsingunum hafi viðhlítandi trúnaðarvottun með hliðsjón af reglugerð þessari og öðrum gildandi reglum sem upplýsingarnar kunna að falla undir.

12. gr.

Fjölföldun trúnaðarskjala, eyðing og aflétting trúnaðar.

Einungis má taka ljósrit af trúnaðarskjölum í viðurkenndum ljósritunarvélum sem ekki eru tölvutengdar og skal blekhylkjum eytt samkvæmt reglum um trúnaðarskjöl.

Ef skjal með trúnaðarstigi *„trúnaðarmál“* eða hærra er fjölfaldað skal skrá fjölda afrita og hverjum þau eru afhent. Ekki skal gera fleiri afrit en nauðsynlegt er.

Afriti trúnaðarskjals skal eytt að lokinni notkun með því að tæta það í viðurkenndum tætara eða brenna.

Ef trúnaðarstig skjals er lækkað eða því aflétt skal strika yfir trúnaðarflokkunina á skjalinu og skrifa dagsetningu og upphafsstafi þess sem ákveður breytinguna, sbr. og 6. gr. Breytingin skal einnig færð inn í skrá yfir trúnaðarflokkaðar upplýsingar.

13. gr.

Trúnaðarskjalasafn og vörslustofnun.

Stofnun eða fyrirtæki, þar sem starfsmenn meðhöndla trúnaðarflokkaðar upplýsingar samkvæmt reglugerð þessari, skal starfrækja sérstakt trúnaðarskjalasafn þar sem tryggt er að slíkar upplýsingar séu meðhöndlaðar samkvæmt reglugerð þessari. Safnið skal halda skrá yfir trúnaðarflokkaðar upplýsingar allan líftíma þeirra frá stofnun eða móttöku þeirra þar til þeim er komið fyrir í varanlegri geymslu eða eytt. Skrá skal móttöku, meðferð, ábyrgðaraðila, dreifingu, vistun og eyðingu trúnaðargagna innan hverrar stofnunar eða fyrirtækis. Takmarka skal aðgang að skránni.

Trúnaðarskjalasafn skal staðsett á öruggu svæði skv. 7. gr. og skal umsjónarmaður þess vera öryggisvottaður að hæsta trúnaðarstigi skjala, sem þar eru geymd, eða því trúnaðarstigi sem öryggisvottun fyrirtækis hefur. Trúnaðarskjalasafni skal haldið aðskildu frá almennu skjalasafni stofnunar eða fyrirtækis. Trúnaðarskjalasöfn skulu sæta úttekt ríkislögreglustjóra á tveggja ára fresti. Stofnanir og fyrirtæki skulu setja sér varðveislustefnu og starfsreglur um rekstur trúnaðarskjalasafna.

Þegar trúnaðarflokkaðar upplýsingar hafa lokið hlutverki sínu skal þeim skilað á sérstakt öryggisskjalasafn ráðherra varnarmála eða eytt í samræmi við reglugerð þessa.

Beiðni um aðgang að trúnaðarflokkuðum upplýsingum skal beint til þess aðila sem þær stafa frá, sbr. merkingu þeirra.

III. KAFLI

Aðgangsheimild.

14. gr.

Veiting aðgangsheimildar.

Forstöðumaður stofnunar eða framkvæmdastjóri fyrirtækis ber ábyrgð á veitingu aðgangsheimildar til handa einstaklingi, sem þarf starfs síns vegna aðgang að trúnaðarflokkuðum upplýsingum, í samræmi við ákvæði reglugerðar þessarar.

Óheimilt er að veita einstaklingi aðgangsheimild að trúnaðarflokkuðum upplýsingum, svæðum, húsnæði, mannvirkjum, búnaði eða öryggissamningum, nema fyrir liggi staðfesting ríkislögreglustjóra á því að viðkomandi hafi fengið útgefna viðeigandi öryggisvottun.

Nú krefst brýn nauðsyn þess, svo sem ríkir almannahagsmunir, að einstaklingur fái veitta aðgangsheimild, þrátt fyrir að ekki liggi fyrir öryggisvottun ríkislögreglustjóra, og er slíkt þá heimilt, enda sé öryggi trúnaðarflokkaðra upplýsinga ekki stefnt í hættu. Tilkynna skal ríkislögreglustjóra þegar í stað um slíkar undanþágur, séu þær veittar.

15. gr.

Aðgangur að trúnaðarflokkuðum upplýsingum.

Áður en einstaklingur fær í hendur trúnaðarflokkaðar upplýsingar, merktar trúnaðarmál eða hærra skal hann hafa fengið viðeigandi öryggisvottun samkvæmt reglugerð þessari. Öryggisvottun einstaklings er ákveðin fyrir tilgreint trúnaðarstig sem skal ekki vera hærra en nauðsynlegt er.

Gögn, sem merkt eru trúnaðarstigi *„trúnaðarmál“* eða hærra, skulu einungis meðhöndluð af aðilum sem hafa öryggisvottun á því stigi eða hærra.

Þó öryggisvottun einstaklings heimili aðgang að ákveðnum gögnum skal aðgangur takmarkast við þau gögn sem nauðsyn krefur.

16. gr.

Aðgangur að svæðum.

Áður en einstaklingur fær aðgang að svæðum, þar sem trúnaðarflokkaðar upplýsingar eru geymdar eða meðhöndlaðar, skal hann hafa fengið viðeigandi öryggisvottun samkvæmt reglugerð þessari, nema gerðar hafi verið sérstakar öryggisráðstafanir til að skýla þeim og hann sé í fylgd öryggisvottaðs einstaklings. Að öðru leyti ákveður forstöðumaður stofnunar eða yfirmaður öryggismála aðgangsheimildir að slíkum svæðum.

Skrá skal nöfn gesta stofnunar, sem fá aðgang að geymslustað trúnaðarflokkaðra upplýsinga eða þeim stað þar sem þær eru meðhöndlaðar, komutíma þeirra og brottfarartíma. Þeir skulu ávallt vera í fylgd öryggisvottaðs einstaklings.

Yfirmaður öryggismála getur heimilað óvottuðum starfsmanni stofnunar aðgang að geymslustað trúnaðarflokkaðra upplýsinga, s.s. vegna viðhalds eða þrifa, enda hafi verið gerðar viðeigandi ráðstafanir til að skýla upplýsingunum eða að fyrrnefndur starfsmaður sé í stöðugri fylgd öryggisvottaðs einstaklings.

17. gr.

Afturköllun aðgangsheimildar.

Aðgangsheimild fellur úr gildi þegar:

a) einstaklingur lætur af störfum sem heimildar var krafist fyrir,
b) þörf fyrir heimild, annarra ástæðna vegna, er ekki lengur fyrir hendi eða
c) viðkomandi hefur ekki lengur gilda öryggisvottun samkvæmt reglugerð þessari.

Komi fram upplýsingar, sem gefa ástæðu til að draga í efa öryggishæfi vottaðs einstaklings, skal forstöðumaður viðkomandi stofnunar eða framkvæmdastjóri fyrirtækis afturkalla aðgangsheimild, takmarka hana eða fella tímabundið úr gildi. Slík ákvörðun skal þegar tilkynnt ríkislögreglustjóra sem metur hvort viðkomandi haldi óbreyttri öryggisvottun.

Nú hefur ríkislögreglustjóri afturkallað öryggisvottun skv. 28. gr. og skal þá aðgangsheimild jafnframt afturkölluð samkvæmt grein þessari.

Ákvörðun forstöðumanns stofnunar eða framkvæmdastjóra fyrirtækis um afturköllun aðgangsheimildar er endanleg.

18. gr.

Aðgangur æðstu stjórnar ríkisins.

Heimilt er að veita forseta Íslands og ráðherrum, sem ekki hafa hlotið öryggisvottun samkvæmt reglugerð þessari, aðgang að trúnaðarflokkuðum upplýsingum. Áður en slíkur aðgangur er veittur skulu þeim kynntar skyldur sínar um trúnað og kvaðir við meðferð trúnaðarflokkaðra upplýsinga samkvæmt reglugerð þessari. Framangreindum aðilum er skylt að gæta fyllsta trúnaðar um þær upplýsingar sem þeim berast á grundvelli þessarar heimildar.

IV. KAFLI
Öryggisvottun og öryggisviðurkenning.

19. gr.

Almennt um öryggisvottun og öryggisviðurkenningu.

Ráðherra varnarmála ber ábyrgð á útgáfu öryggisvottana og öryggisviðurkenninga samkvæmt reglugerð þessari. Ríkislögreglustjóri gefur út öryggisvottanir og öryggisviðurkenningar sem öryggisstjórnvald, í umboði ráðherra varnarmála, samkvæmt reglugerð þessari.

20. gr.

Öryggisvottun einstaklings.

Áður en einstaklingur fær öryggisvottun skal hann hafa staðist bakgrunnsskoðun, undirrita drengsskaparheit sem lýtur að þagmælsku varðandi þær trúnaðarflokkuðu upplýsingar sem hann fær aðgang að í starfi og fá kynningu á reglum um meðferð trúnaðarflokkaðra upplýsinga af hálfu ríkislögreglustjóra. Þagnarskylda helst þótt látið sé af starfi eða verkefni ljúki.

Bakgrunnsskoðun yfirvalda í öðru ríki skal viðurkennd hér á landi ef þess er óskað og hún er staðreynd með viðeigandi gögnum. Við ákvörðun um öryggisvottun í slíkum tilvikum skal lagt mat á bakgrunnsskoðun öryggisstjórnvalds heimaríkis viðkomandi einstaklings.

Ríkislögreglustjóri getur ákveðið að einstaklingur, sem hlotið hefur bakgrunnsskoðun í öðru ríki, skuli engu að síður gangast undir bakgrunnsskoðun hér á landi áður en hann fær útgefna öryggisvottun samkvæmt reglugerð þessari.

Hver sú stofnun eða fyrirtæki, sem hefur öryggisvottaða einstaklinga að störfum, skal halda uppfærða skrá yfir öryggisvottaða starfsmenn sína. Skrá skal gildistíma öryggisvottunar, trúnaðarstig, hvort vottun sé útrunnin, hafi verið afturkölluð, tímabundið afturkölluð eða sé í afgreiðslu.

Yfirmaður öryggismála ber ábyrgð á að starfsmenn, sem þess þurfa, séu ávallt með gilda vottun að réttu trúnaðarstigi.

21. gr.

Öryggisvottun fyrirtækis.

Fyrirtæki, þ.m.t. birgir, þjónustuaðili, útboðsaðili, verktaki eða útflytjandi, þar sem starfsmenn hafa aðgang að trúnaðarflokkuðum upplýsingum, eða aðstöðu þar sem trúnaðarflokkaðar upplýsingar eru geymdar eða meðhöndlaðar, skal öryggisvottað. Þannig skulu stjórnar- og yfirmenn slíks fyrirtækis, ásamt yfirmanni öryggismála, standast öryggisvottun skv. 20. gr.

Til grundvallar útgáfu öryggisvottunar fyrir fyrirtæki skal liggja beiðni frá innkaupastofnun (verkkaupa) sem kaupir vöru eða þjónustu af fyrirtækinu (verksala). Umsókn innkaupastofnunar um öryggisvottun fyrirtækis skal vera á þar til gerðu eyðublaði sem ríkislögreglustjóri útfærir. Þá skal einnig liggja fyrir öryggissamningur milli innkaupastofnunar og fyrirtækis, sbr. 25. gr. Innkaupastofnun getur óskað nýrrar öryggisvottunar fyrir fyrirtæki og/eða hækkunar á trúnaðarstigi öryggisvottunar sem fyrirtæki hefur þegar hlotið.

Áður en starfsmaður fyrirtækis fær aðgang að trúnaðarflokkuðum upplýsingum að trúnaðarstiginu *„trúnaðarmál“* eða hærra eða ef slíkt er talið nauðsynlegt af öðrum ástæðum, skal hann öryggisvottaður að viðeigandi trúnaðarstigi.

Öryggisvottun fyrir fyrirtæki skal ekki gefin út ef réttmætur efi er um öryggishæfi fyrirtækisins eða starfsmanna þess. Eingöngu skal leggja mat á tengsl sem varða hæfi fyrirtækis eða starfsmanna þess og vilja til að framfylgja fyrirbyggjandi öryggisráðstöfunum samkvæmt ákvæðum í reglugerð þessari. Við það mat skal framkvæma bakgrunnsskoðun á stjórnar- og yfirmönnum fyrirtækisins í samræmi við 30. gr., sbr. 31. og 32. gr.

Fyrirtæki skal veita allar upplýsingar sem taldar eru mikilvægar fyrir mat á öryggishæfi þess eða starfsmanna þess m.t.t. ákvörðunar öryggisvottunar.

Framkvæmdastjóri fyrirtækis skal tafarlaust tilkynna ríkislögreglustjóra:

a) verði breytingar á skipun stjórnarmanna og/eða yfirmanna,
b) færist eignarhald fyrirtækisins til nýrra aðila,
c) verði starfsemi eða búnaður fluttur,
d) verði breyting gerð á húsnæði, aðstöðu eða búnaði sem áður hefur verið öryggisviðurkenndur,

e) verði fyrirtækinu veitt heimild til greiðslustöðvunar, til að leita nauðasamninga eða nauðasamninga til greiðsluaðlögunar eða verði bú þess tekið til gjaldþrotaskipta eða
f) verði önnur atriði til þess að hafa hugsanleg áhrif á öryggishæfi fyrirtækis samkvæmt reglugerð þessari.

Komi upp aðstæður hjá fyrirtæki, sem gætu ógnað öryggi samkvæmt reglugerð þessari og ekki er hægt að draga úr ógninni með fyrirbyggjandi öryggisráðstöfunum, getur ríkislögreglustjóri afturkallað öryggisvottun viðkomandi fyrirtækis í samræmi við ákvæði 28. gr.

Trúnaðarflokkaðar upplýsingar eða búnað, sem þær eru vistaðar á, má ekki færa yfir til nýrra eigenda fyrirtækis, nema fyrir liggi öryggisvottun ríkislögreglustjóra á nýjum eiganda samkvæmt reglugerð þessari. Búnað má þó færa yfir til nýrra eigenda hafi trúnaðarflokkuðum upplýsingum verið eytt af umræddum búnaði í samræmi við reglugerð þessa.

Ráðherra getur gert öryggissamninga við aðila hérlendis (útflytjendur) sem þurfa öryggisvottun til þess að stunda milliríkjaviðskipti. Ákvæði þessarar greinar sem og ákvæði 25. gr. skulu gilda um slíka samninga að breyttu breytanda.

Óheimilt er að gefa út öryggisvottun til handa fyrirtæki, þ.m.t. birgjum, þjónustuaðilum, útboðsaðilum, verktökum eða útflytjendum, nema starfsmenn þess, sem koma til með að meðhöndla trúnaðarflokkaðar upplýsingar samkvæmt reglugerð þessari, hafi staðist bakgrunnsskoðun skv. 30. gr., sbr. 31. og 32. gr. og, eftir atvikum, aðstaða fyrirtækisins uppfylli skilyrði 7. og 23. gr.

22. gr.

Öryggisviðurkenning upplýsingakerfis og búnaðar.

Áður en trúnaðarflokkaðar upplýsingar eru meðhöndlaðar, hýstar eða þeim miðlað í öruggu upplýsingakerfi skal ríkislögreglustjóri viðurkenna kerfið að viðeigandi trúnaðarstigi.

Ríkislögreglustjóri getur falið öðrum aðilum, sem hlotið hafa viðeigandi vottun, að sinna öryggisþjónustu við upplýsingakerfi sem trúnaðarflokkaðar upplýsingar eru meðhöndlaðar í.

Búnaður, tæki og verkferlar vegna eyðingar trúnaðarflokkaðra upplýsinga, sbr. 12. gr., skulu viðurkennd af ríkislögreglustjóra.

Óheimilt er að gefa út öryggisviðurkenningu fyrir upplýsingakerfi eða búnað nema það eða hann uppfylli öryggisstaðla viðkomandi kerfis og kröfur.

23. gr.

Öryggisviðurkenning aðstöðu.

Ríkislögreglustjóri gefur út öryggisviðurkenningar fyrir húsnæði, svæði og aðstöðu til handa þeim sem meðhöndla og varðveita trúnaðarflokkaðar upplýsingar samkvæmt reglugerð þessari. Slíkt húsnæði, svæði eða aðstaða skal uppfylla skilyrði um lágmarksöryggi og standast öryggisviðurkenningu, sbr. 7. gr.

24. gr.

Gildistími öryggisvottunar og -viðurkenningar.

Gildistími öryggisvottunar fyrir einstakling er sem hér segir:
a) eitt ár sé um að ræða fyrstu öryggisvottun,
b) tvö til fimm ár, samkvæmt ákvörðun ríkislögreglustjóra, sé um endurnýjun að ræða eða
c) fimm ár sé um að ræða endurnýjun öryggisvottunar fyrir fastráðinn opinberan starfsmann sem meðhöndlar trúnaðarflokkaðar upplýsingar að jafnaði.

Gildistími öryggisvottunar fyrir fyrirtæki er sem hér segir:
a) tvö ár sé um fyrstu öryggisvottun að ræða eða
b) þrjú til fimm ár, samkvæmt ákvörðun ríkislögreglustjóra, sé um endurnýjun að ræða.

Ákveða má annan gildistíma öryggisvottunar en segir í a- og b-lið til samræmis við gildistíma öryggissamnings.

Gildistími öryggisviðurkenningar fyrir upplýsingakerfi og búnað er sem hér segir:
a) bráðabirgðaviðurkenning *(Interim Approval to Operate (IATO))* sem gildir lengst í tólf mánuði eða
b) öryggisviðurkenning sem gildir lengst í þrjú ár.

Gildistími öryggisviðurkenningar fyrir aðstöðu er til þriggja ára, nema breytingar verði gerðar á henni. Þó er heimilt að veita stofnunum öryggisviðurkenningu fyrir aðstöðu til lengri tíma og jafnvel ótímabundið, eftir atvikum, mæli sérstakar ástæður með því.

Gildistími öryggisvottunar og/eða -viðurkenningar skal koma skýrt fram við útgáfu hennar.

Öryggisvottun fellur úr gildi þegar:

a) gildistími hennar er liðinn,
b) öryggissamningur skv. 25. gr. rennur út eða gildistíma verkefnis lýkur,
c) einstaklingur, sem öryggisvottunar var krafist fyrir, lætur af störfum,
d) fyrirtæki verður tekið til gjaldþrotaskipta eða hættir starfsemi eða
e) þörf eða forsendur fyrir öryggisvottun, annarra ástæðna vegna, eru ekki lengur fyrir hendi.

Öryggisviðurkenning fellur úr gildi þegar:

a) gildistími hennar er liðinn,
b) upplýsingakerfi og búnaður uppfylla ekki lengur kröfur samkvæmt reglugerð þessari,
c) aðstöðu fyrirtækis eða stofnunar hefur verið breytt eða hún uppfyllir ekki lengur kröfur samkvæmt reglugerð þessari,
d) fyrirtæki, þar sem búnaður er, verður gjaldþrota eða hættir starfsemi eða
e) þörf fyrir öryggisviðurkenningu, annarra ástæðna vegna, er ekki lengur fyrir hendi.

25. gr.

Öryggissamningur.

Stofnun, sem geymir trúnaðarflokkaðar upplýsingar samkvæmt reglugerð þessari, skal gera öryggissamning við birgja og þjónustuaðila sem viðskiptanna vegna þurfa aðgang að slíkum upplýsingum. Slíkir samningar eru grundvöllur öryggisvottunar ríkislögreglustjóra á fyrirtækjum skv. 21. gr. fyrir viðeigandi trúnaðarstig, ef við á.

Ríkislögreglustjóri getur ákveðið að öryggissamningur skv. 1. mgr. skuli gerður ef birgir eða þjónustuaðili þarf aðgang að öryggisvottuðu tölvukerfi eða geymslustað eða ef talin er þörf á öryggissamningi af öðrum ástæðum. Öryggissamningur skal gerður áður en birgir eða þjónustuaðili fær aðgang að trúnaðarflokkuðum upplýsingum.

Í öryggissamningi, sem skal vera viðauki við verksamning vegna öryggisflokkaðra vöru- eða þjónustukaupa eða útboðs, skal kveðið á um ábyrgð og skyldur samkvæmt reglugerð þessari, þ.m.t. varðandi:

a) trúnaðarstig viðskiptanna, sérstaklega tilgreint fyrir einstaka þætti verkefnisins,
b) framkvæmd bakgrunnsskoðunar á birgi eða þjónustuaðila og annars eftirlits til að meta öryggisþætti og að birgir eða þjónustuaðili framfylgi öryggisákvæðum samningsins sem og öðrum skyldum samkvæmt reglugerð þessari,
c) gildistíma öryggissamnings, ef við á, og
d) afleiðingar brots á öryggissamningnum, þ.m.t. samningsbundnar sektir.

Útgjöld eða kröfur, sem birgir eða þjónustuaðili hefur undirgengist eða fullnægir þegar hann uppfyllir ákvæði í reglugerð þessari eða ákvæði þeim tengd sem eru samþykkt í öryggissamningi, eru innkaupastofnuninni eða ríkislögreglustjóra óviðkomandi, nema annað sé sérstaklega tilgreint í öryggissamningi.

26. gr.

Synjun um öryggisvottun einstaklings.

Tilkynna skal einstaklingi, sem sótt hefur verið um öryggisvottun fyrir, um niðurstöðu bakgrunnsskoðunar, skv. 30. gr., sbr. 31. og 32. gr., eins fljótt og kostur er. Óheimilt er að veita einstaklingi öryggisvottun standist hann ekki viðmiðanir við mat á ákvörðun öryggisvottunar skv. 31. og 32. gr. að mati ríkislögreglustjóra.

Með synjun á öryggisvottun skal fara að málsmeðferðarreglum stjórnsýslulaga. Komist ríkislögreglustjóri að þeirri niðurstöðu að synja beri einstaklingi um öryggisvottun á grundvelli bakgrunnsskoðunar skal ríkislögreglustjóri upplýsa viðkomandi einstakling um fyrirhugaða synjun og rökstuddar ástæður hennar. Með þeim rökstuðningi skulu þó ekki koma fram upplýsingar, sem mikilvægt er að leynt skuli fara, þar sem þær:

a) eru mikilvægar eða geta verið skaðlegar fyrir öryggi Íslands eða samstarfsríki þess, tengsl við erlend stjórnvöld eða aðra mikilvæga öryggishagsmuni ríkisins,
b) eru mikilvægar til þess að vernda uppruna heimilda,
c) varða tengsl hans við einstaklinga, sem standa honum nærri, sem ekki er æskilegt að viðkomandi fái upplýsingar um,
d) varða tæknibúnað, framleiðsluupplýsingar, viðskiptagreiningu eða -reikning, viðskiptaleyndarmál eða eru þess eðlis að aðrir geti nýtt sér upplýsingarnar í starfsemi sinni eða
e) varða sakamál eða lögreglurannsókn sem viðkomandi tengist á einhvern máta og ekki er unnt að opinbera.

Einstaklingi skal veittur réttur til andmæla, í samræmi við ákvæði stjórnsýslulaga, áður en ákvörðun er tekin um synjun öryggisvottunar.

Komist ríkislögreglustjóri að þeirri niðurstöðu, eftir að einstaklingi hefur verið gefinn kostur á að njóta andmælaréttar, að synja beri um útgáfu öryggisvottunar, skal sú ákvörðun tilkynnt viðkomandi einstaklingi sem og beiðanda bakgrunnsskoðunar með formlegum hætti. Ákvörðun ríkislögreglustjóra um synjun öryggisvottunar skal ávallt rökstudd, sbr. þó 2. mgr., í samræmi við ákvæði stjórnsýslulaga. Beiðanda bakgrunnsskoðunar skal þó einungis tilkynnt að synjað hafi verið um öryggisvottun á grundvelli reglugerðar þessarar án rökstuðnings eða frekari skýringa. Í ákvörðun ríkislögreglustjóra skal leiðbeint um heimild til að senda kæru til ráðherra varnarmála í samræmi við ákvæði stjórnsýslulaga.

Aðili máls á rétt á því að kynna sér skjöl og önnur gögn er málið varða, í samræmi við ákvæði stjórnsýslulaga, með þeim undantekningum sem þar greinir. Þá er ríkislögreglustjóra heimilt, þegar sérstaklega stendur á, að takmarka aðgang málsaðila að gögnum ef hagsmunir hans af því að notfæra sér vitneskju úr þeim þykja eiga að víkja fyrir mun ríkari almanna- eða einkahagsmunum, sbr. ákvæði stjórnsýslulaga. Við slíkt mat skal meðal annars taka tillit til þeirra atriða sem tilgreind eru í 2. mgr. Meta verður sérstaklega í hverju tilviki þau sjónarmið sem fyrir liggja í hlutaðeigandi máli.

27. gr.

Synjun um öryggisvottun fyrirtækis.

Tilkynna skal forsvarsmanni stofnunar eða framkvæmdastjóra fyrirtækis, sem óskað hefur eftir öryggisvottun fyrirtækis, um niðurstöðu skoðunar, skv. 21.-23. gr., sbr. 7. gr., eins fljótt og kostur er. Óheimilt er að veita fyrirtæki eða stofnun, aðstöðu, upplýsingakerfi eða búnaði öryggisviðurkenningu og/eða -vottun fyrirtækis sé viðmiðunum, skv. 21.-23. gr., sbr. 7. gr., ekki fullnægt að mati ríkislögreglustjóra.

Sé fyrirhugað að synja um öryggisvottun fyrirtækis skal fara að málsmeðferðarreglum stjórnsýslulaga, hvað varðar rétt aðila til rökstuðnings og andmæla, áður en endanleg ákvörðun er tekin.

Komist ríkislögreglustjóri að þeirri niðurstöðu að synja beri um útgáfu öryggisvottunar fyrirtækis skal sú ákvörðun tilkynnt forsvarsmanni stofnunar eða framkvæmdastjóra fyrirtækis.

28. gr.

Afturköllun öryggisvottunar.

Yfirmaður öryggismála skal, þegar í stað, tilkynna ríkislögreglustjóra um starfslok einstaklings, sem hlotið hefur öryggisvottun samkvæmt reglugerð þessari, eða að ekki sé lengur þörf fyrir öryggisvottun viðkomandi starfsmanns. Ríkislögreglustjóri skal þá þegar afturkalla öryggisvottun hans.

Yfirmaður öryggismála skal jafnframt þegar í stað tilkynna ríkislögreglustjóra um breytta aðstöðu í fyrirtæki, svo sem breytingu á eignarhaldi, fjárhagsstöðu, húsnæði, svæði, starfsmönnum eða öðru því sem máli kann að skipta og gæti haft áhrif á öryggishæfi fyrirtækisins eða starfsmanna þess til að njóta öryggisvottunar. Ríkislögreglustjóri skal þá þegar meta hvort efni sé til að afturkalla öryggisvottun viðkomandi fyrirtækis og skal afturköllun öryggisvottunar þá framkvæmd í samræmi við grein þessa eftir atvikum.

Nú er gildistími öryggisvottunar runninn út og skal ríkislögreglustjóri þá tilkynna viðkomandi einstaklingi og yfirmanni öryggismála viðkomandi stofnunar eða fyrirtækis um útrunna öryggisvottun.

Komi fram upplýsingar, sem geta haft áhrif á öryggishæfi öryggisvottaðs einstaklings, skal slíkt þegar í stað tilkynnt ríkislögreglustjóra sem metur hvort fella eigi tímabundið niður eða afturkalla öryggisvottun viðkomandi og hefja frekari athugun á málinu.

Ákveði ríkislögreglustjóri að afturkalla öryggisvottun eða fella öryggisvottun tímabundið niður, skal það þegar í stað tilkynnt viðkomandi einstaklingi, fyrirtæki eða stofnun sem sótti um vottun fyrir viðkomandi.

Fylgja skal málsmeðferðarreglum 26. gr. við afturköllun öryggisvottunar einstaklings. Ríkislögreglustjóri getur afturkallað öryggisvottun tímabundið á meðan kærumeðferð máls fer fram skv. 38. gr.

Framkvæmdastjóra fyrirtækis skal tilkynnt um fyrirhugaða afturköllun öryggisvottunar og ástæður hennar og veittur kostur á að neyta andmælaréttar í samræmi við ákvæði stjórnsýslulaga. Endanleg ákvörðun ríkislögreglustjóra um afturköllun öryggisvottunar fyrirtækis skal rökstudd í samræmi við ákvæði stjórnsýslulaga.

29. gr.

Afturköllun öryggisviðurkenningar.

Yfirmaður öryggismála skal þegar í stað tilkynna ríkislögreglustjóra um breytingar sem orðið hafa á upplýsingakerfi, búnaði, aðstöðu eða rými fyrirtækis eða stofnunar, sem hlotið hefur öryggisviðurkenningu samkvæmt reglugerð þessari, eða ef ekki er lengur þörf fyrir viðkomandi öryggisviðurkenningu. Ríkislögreglustjóri skal þá þegar afturkalla umrædda öryggisviðurkenningu eftir atvikum.

Nú er gildistími öryggisviðurkenningar runninn út og skal ríkislögreglustjóri þá þegar tilkynna yfirmanni öryggismála viðkomandi stofnunar eða fyrirtækis þar um.

Komi fram upplýsingar, sem geta haft áhrif á öryggisviðurkenningu samkvæmt reglugerð þessari, skal slíkt þegar tilkynnt ríkislögreglustjóra sem metur hvort fella eigi tímabundið niður eða afturkalla umrædda öryggisviðurkenningu og hefja frekari athugun á málinu.

Ákveði ríkislögreglustjóri að fella niður öryggisviðurkenningu eða afturkalla hana tímabundið skal það þegar í stað tilkynnt yfirmanni öryggismála viðkomandi stofnunar eða fyrirtækis sem sótti um viðurkenningu.

Forstöðumanni stofnunar eða framkvæmdastjóra fyrirtækis skal tilkynnt um fyrirhugaða afturköllun öryggisvottunar og ástæður hennar og veittur kostur á að neyta andmælaréttar í samræmi við ákvæði stjórnsýslulaga. Endanleg ákvörðun ríkislögreglustjóra um afturköllun öryggisvottunar stofnunar eða fyrirtækis skal rökstudd í samræmi við ákvæði stjórnsýslulaga.

V. KAFLI
Bakgrunnsskoðun.

30. gr.

Framkvæmd bakgrunnsskoðunar á einstaklingi.

Ríkislögreglustjóri framkvæmir bakgrunnsskoðun á einstaklingi samkvæmt beiðni þess sem ber ábyrgð á að veita aðgangsheimild skv. III. kafla. Ráðherra ákveður hvaða fyrirtæki eða stofnanir eru bær eða bærar til að óska eftir öryggisvottunum samkvæmt reglugerð þessari.

Bakgrunnsskoðun getur m.a. falist í skoðun á viðkomandi einstaklingi í skrám lögreglu, þ.m.t. málaskrá lögreglu, skoðun á sakavottorði, upplýsingakerfi Interpol, SIS-upplýsingakerfinu, upplýsingum úr Þjóðskránni, eftir atvikum fyrirspurnum til erlendra yfirvalda, skoðun hjá tollyfirvöldum, héraðsdómi og í öðrum opinberum skrám.

Vegna útgáfu öryggisvottunar að trúnaðarstigunum *„trúnaðarmál“* og *„leyndarmál“* skal bakgrunnsskoða a.m.k. fimm ár aftur í tímann. Vegna útgáfu öryggisvottunar að trúnaðarstiginu *„algjört leyndarmál“* skal bakgrunnsskoða a.m.k. tíu ár aftur í tímann.

Við bakgrunnsskoðun skal meta upplýsingar sem einstaklingur hefur sjálfur veitt, ríkislögreglustjóri býr yfir og eftir atvikum úr opinberum skrám, sbr. 2. mgr. Stofnunum, sem ríkislögreglustjóri óskar upplýsinga frá vegna bakgrunnsskoðunar, ber skylda til að miðla upplýsingum úr skrám sínum til ríkislögreglustjóra. Upplýsingum úr skrám skal miðlað skriflega eða rafrænt. Bakgrunnsskoðun getur einnig náð til annarra heimilda, þ.m.t. upplýsinga frá vinnustað, opinberum

stofnunum og eftir atvikum frá öðrum heimildum. Upplýsingar, sem aflað er við bakgrunnsskoðun, skulu afhentar ríkislögreglustjóra án endurgjalds.

Bakgrunnsskoðun skal ekki framkvæmd nema viðkomandi einstaklingi hafi verið gerð grein fyrir þörfinni á henni og hvar upplýsinga verði aflað og formlegt samþykki hans liggi fyrir á þar til gerðu eyðublaði ríkislögreglustjóra. Með samþykki sínu gengst viðkomandi undir að gefa fullnægjandi og réttar upplýsingar, m.a. um tengsl sem kunna að hafa áhrif á mat á öryggishæfi.

Bakgrunnsskoðun skal vera ítarlegri eftir því sem trúnaðarstig hækkar. Við öryggisvottun fyrir *„leyndarmál“* eða hærra trúnaðarstig eða í öðrum sérstökum tilfellum, getur bakgrunnsskoðunin náð til einstaklinga, sem eru tengdir viðkomandi fjölskylduböndum eða eru í sambýli við hann, enda hafi þeir einstaklingar veitt upplýst samþykki.

Upplýsingar, sem veittar eru ríkislögreglustjóra í tengslum við bakgrunnsskoðanir, skulu ekki nýttar í öðrum tilgangi en til öryggisvottunar samkvæmt reglugerð þessari. Tryggja skal að eingöngu þeir starfsmenn sem sinna öryggisvottun hafi aðgang að þeim upplýsingum.

31. gr.

Viðmiðanir við ákvörðun um öryggisvottun einstaklings.

Öryggisvottun skal eingöngu útgefin eða endurnýjuð ef viðkomandi einstaklingur stenst bakgrunnsskoðun skv. 30. gr., samanber og þau viðmið sem sett eru í þessari grein, sbr. og 32. gr. Við mat á öryggishæfi einstaklings til að meðhöndla trúnaðarflokkaðar upplýsingar skal taka mið af eftirtöldum þáttum, m.t.t. áreiðanleika, heiðarleika og dómgreindar viðkomandi einstaklings:

a) hafi hann tengst skemmdarverkum, njósnum eða skipulagningu þeirra, sýndum tilræðum eða öðrum slíkum athöfnum,
b) hafi hann framið refsivert athæfi eða brot eða hvatt til slíkra athafna,
c) sé um að ræða tengsl sem geta leitt til þess að viðkomandi sjálfur eða nákominn ættingi sæti hótunum er ógna lífi, heilsu, friðhelgi eða virðingu og hann þvingaður til athafna sem gætu ógnað öryggi trúnaðarflokkaðra upplýsinga,
d) hafi hann gefið falsaðar eða rangar upplýsingar eða að vísvitandi sé þagað um upplýsingar sem viðkomandi mátti vita að hefðu áhrif á niðurstöðu mats um útgáfu öryggisvottunar,
e) eigi hann að baki sögu um misnotkun áfengis eða annarra vímugjafa,
f) eigi hann við sjúkdóma að stríða sem vegna lyfjagjafar geta haft áhrif á áreiðanleika, heiðarleika eða dómgreind,
g) hafi hann átt hlut í að trúnaðarflokkuðum upplýsingum sé stofnað í hættu, að um brot á öryggisreglum sé að ræða, hafi viðkomandi neitað að gefa persónuupplýsingar um sig, heimili ríkislögreglustjóra ekki að gera þær athuganir sem teljast mikilvægar og nauðsynlegar við bakgrunnsskoðun, neiti að heita trúnaði, gefi til kynna að hann vilji ekki vera bundinn þagnarskyldu eða neiti að mæta í viðtal sem ríkislögreglustjóri hefur boðað hann til,
h) sé um að ræða efnahagslega þætti sem geta leitt til óheiðarleika,
i) hvort um sé að ræða tengsl hans við einstaklinga eða aðila, svo sem samtök, fyrirtæki, félög eða hópa innanlands eða erlendis sem hafa ólögleg markmið, geta ógnað lýðræðislegu samfélagi eða tengjast skipulagningu, undirbúningi eða framkvæmd á skipulagðri glæpastarfsemi, fíkniefnamisferli, njósnum, skemmdar- eða hryðjuverkum,
j) ófullnægjandi tækifæri séu til að framkvæma bakgrunnsskoðun,
k) sé um að ræða tengsl viðkomandi við erlend ríki og
l) öðrum þáttum sem geta gefið tilefni til gruns um að viðkomandi gæti haft í frammi háttsemi sem ógnað geti öryggishagsmunum samkvæmt reglugerð þessari.

Ákvörðun um að veita öryggisvottun eða ákvörðun um synjun hennar, sbr. 26. gr., skal byggjast á upplýstu, skýru, málefnalegu og einstaklingsmiðuðu, alhliða mati á fyrirliggjandi upplýsingum. Pólitísk tengsl, þ.m.t. þátttaka í löglegum stjórnmálasamtökum eða stofnunum eða hvers kyns löglegum félögum skulu ekki hafa áhrif á hæfismat viðkomandi vegna öryggisvottunar. Eingöngu skal taka tillit til neikvæðra upplýsinga um nákomna einstaklinga ef tengsl þeirra eru talin þess eðlis að þau hafi áhrif á háttsemi og öryggishæfi þess sem á að öryggisvotta.

Ekki skal gefa út öryggisvottun fyrr en viðkomandi hefur hlotið viðeigandi fræðslu af hálfu öryggisstjórnvalds. Í sérstökum tilvikum getur ríkislögreglustjóri sett önnur málefnaleg skilyrði fyrir öryggisvottun.

32. gr.

Mat á afbrotaferli.

Nú hefur komið í ljós við bakgrunnsskoðun skv. 30. og 31. gr. að einstaklingur hefur gerst brotlegur við lög eða er grunaður um að hafa gerst brotlegur við lög og er ríkislögreglustjóra þá heimilt að leggja til grundvallar viðmið samkvæmt þessari grein við ákvörðun um það hvort gefa eigi út öryggisvottun til handa viðkomandi einstaklingi eða ekki.

Við ákvörðun um hvort gefa eigi út öryggisvottun til handa einstaklingi skal sérstaklega athuga brotaferil hans. Leggja skal til grundvallar upplýsingar úr sakaskrá og eftir atvikum málaskrá og öðrum skrám lögreglu um viðkomandi einstakling, sbr. 30. gr.

Hafi einstaklingur, hérlendis eða erlendis, sætt sektum eða verið dæmdur til refsingar eða eigi ólokið máli í refsivörslukerfinu, þar sem hann er grunaður eða sakaður um refsiverða háttsemi samkvæmt íslenskum lögum, skal ríkislögreglustjóri synja honum um útgáfu öryggisvottunar, enda séu brotin stórfelld eða gefi vísbendingar um að öryggi ríkisins og/eða almannahagsmunum kunni að stafa hætta af.

Ríkislögreglustjóra er jafnframt skylt að synja um útgáfu öryggisvottunar hafi einstaklingur verið dæmdur fyrir alvarleg brot, svo sem brot á almennum hegningarlögum, notkun eða dreifingu ávana- og fíkniefna, ólögmæta notkun eða dreifingu vopna, stórfellt tollalagabrot, brot sem stefnt hefur lífi einhvers í hættu, ofbeldisbrot, fjárkúgun, brot sem ógna öryggi ríkisins, kynferðisbrot, sé eða hafi verið meðlimur í ólöglegum samtökum eða meintum glæpasamtökum.

Ríkislögreglustjóri getur ákveðið að synja beri einstaklingi um útgáfu öryggisvottunar á grundvelli annarra brota en talin eru í grein þessari, enda liggi málefnalegar ástæður fyrir.

Ennfremur er heimilt að taka tillit til eftirfarandi atvika:

a) komin er fram kæra á hendur einstaklingi fyrir refsivert brot, sem ætla má að varði fangelsisrefsingu eða
b) einstaklingur er eftirlýstur af lögreglu, gefin hefur verið út handtökuskipun á hendur honum eða lagt á hann farbann samkvæmt ákvæðum laga um meðferð sakamála, nr. 88/2008.

Komi í ljós við bakgrunnsskoðun, skv. 30. og 31. gr., að lögregla hafi þurft að hafa endurtekin afskipti af einstaklingi vegna meintra brota af hans hálfu, getur ríkislögreglustjóri ákveðið að synja útgáfu öryggisvottunar honum til handa.

33. gr.

Endurtekning bakgrunnsskoðunar.

Ríkislögreglustjóra er heimilt að endurtaka bakgrunnsskoðun á einstaklingi að eigin frumkvæði eða að beiðni þar til bærs aðila og með upplýstu samþykki viðkomandi einstaklings. Ríkislögreglustjóra er í slíkum tilvikum heimilt að leggja til grundvallar gögn og upplýsingar sem þegar liggja fyrir, eftir því sem kostur er, en jafnframt óska frekari gagna og upplýsinga ef þörf er á.

Að auki er ríkislögreglustjóra heimilt, að eigin frumkvæði eða samkvæmt beiðni þar til bærs aðila, að gera úrtaksathugun á þeim aðilum sem staðist hafa bakgrunnsskoðun eins lengi og öryggisvottanir þeirra eru í gildi.

VI. KAFLI
Ýmis ákvæði.

34. gr.

Upplýsingaskylda einstaklings.

Einstaklingur, sem hefur fengið öryggisvottun samkvæmt reglugerð þessari, skal upplýsa yfirmann öryggismála um allt það sem kann að hafa áhrif á öryggishæfi hans. Yfirmaður öryggismála skal þá þegar tilkynna það ríkislögreglustjóra sem metur hvort tilefni sé til að afturkalla öryggisvottun viðkomandi einstaklings skv. 28. gr.

35. gr.

Nánar um framkvæmd.

Við framkvæmd reglugerðar þessarar skal taka mið af, að breyttu breytanda:

a) skjali Atlantshafsráðsins nr. C-M(2002)49 frá 17. júní 2002 um öryggi innan Atlantshafsbandalagsins,
b) ákvörðun ráðsins (ESB) nr. 2011/292/ESB frá 31. mars 2011 um öryggisreglur til verndar trúnaðarflokkuðum upplýsingum ESB og
c) öðrum alþjóðasamningum og reglum til nánari útfærslu þeirra, eftir því sem við á.

36. gr.

Þagnarskylda.

Starfsmenn ríkislögreglustjóra skulu gæta trúnaðar um allar upplýsingar sem fram koma við bakgrunnsskoðun og leynt skulu fara.

Aðgangur starfsmanna ríkislögreglustjóra að trúnaðarflokkuðum upplýsingum skv. 1. mgr. ræðst af störfum þeirra innan lögreglunnar.

Þeir einstaklingar sem, starfa sinna vegna, fá vitneskju um niðurstöðu bakgrunnsskoðunar ríkislögreglustjóra um einstakling skulu gæta fyllsta trúnaðar um efni hennar.

Þeir einstaklingar, verktakar eða aðrir aðilar sem, starfa sinna vegna, fá aðgang að trúnaðarflokkuðum upplýsingum, skulu gæta fyllsta trúnaðar um efni þeirra. Þeir mega ekki, að viðlagðri ábyrgð, skýra óviðkomandi frá því sem þeir komast að í starfi sínu og leynt á að fara.

Þagnarskylda helst þótt látið sé af starfi eða verksamningi ljúki.

37. gr.

Öryggisúttektir ríkislögreglustjóra.

Ríkislögreglustjóri hefur eftirlit með þeim þáttum öryggismála stofnana og fyrirtækja sem varða framkvæmd reglugerðar þessarar, þ.m.t. að þær og þau uppfylli skyldur samkvæmt lögum og reglugerðum, og gefur fyrirmæli um úrbætur.

Ríkislögreglustjóri framkvæmir reglubundnar úttektir á aðstöðu, svæðum, húsnæði, mannvirkjum, tækjum, upplýsingakerfum eða búnaði og öðrum hlutum í eigu, notkun eða sem eru á annan máta undir stjórn stofnunar eða fyrirtækis, í þeim tilgangi að meta hvort óviðkomandi aðilar geti, með eða án tæknilegrar aðstoðar, séð, hlustað á eða lesið trúnaðarflokkaðar upplýsingar.

Ríkislögreglustjóri skal hafa óhindraðan aðgang að hverju því svæði sem trúnaðarflokkaðar upplýsingar eða búnaður til meðferðar trúnaðarflokkaðra upplýsinga er hýstur á, svo unnt sé að framkvæma öryggisúttekt með fullnægjandi hætti.

Komi í ljós, við öryggisúttekt ríkislögreglustjóra samkvæmt grein þessari, að stofnun eða fyrirtæki uppfyllir ekki lengur skyldur samkvæmt lögum eða reglugerð þessari eða að gera þarf athugasemdir við tiltekin atriði, skal ríkislögreglustjóri senda skýrslu þar að lútandi til viðkomandi aðila, eins fljótt og unnt er að úttekt lokinni. Skal aðila gefinn hæfilegur frestur til úrbóta að mati ríkislögreglustjóra. Séu úrbætur ekki gerðar innan frestsins getur ríkislögreglustjóri afturkallað öryggisvottun og/eða -viðurkenningu á grundvelli reglugerðar þessarar og tilkynnt um það til viðeigandi alþjóðastofnunar eftir atvikum.

Öryggisúttektir skal að meðaltali framkvæma á 24 mánaða fresti. Ríkislögreglustjóri setur verklagsreglur um öryggisúttektir samkvæmt grein þessari.

38. gr.

Kæruheimild.

Nú er öryggisvottun einstaklings synjað á grundvelli bakgrunnsskoðunar, sbr. 26. gr., eða öryggisvottun einstaklings afturkölluð, sbr. 28. gr., og má kæra þá ákvörðun til ráðherra varnarmála í samræmi við ákvæði stjórnsýslulaga.

39. gr.
Viðurlög.

Brot á reglugerð þessari varða refsingu samkvæmt eftirfarandi ákvæðum nema þyngri refsing liggi við samkvæmt öðrum lögum:

a) XIV. og XVII. kafla almennra hegningarlaga, nr. 19/1940,
b) 28. gr. varnarmálalaga, nr. 34/2008 og/eða
c) 13. gr. laga um eftirlit með þjónustu og hlutum sem geta haft hernaðarlega þýðingu, nr. 58/2010.

40. gr.
Gildistaka o.fl.

Reglugerð þessi er sett skv. 24. og 27. gr. varnarmálalaga, nr. 34/2008, og með tilliti til 15. og 18. gr. laga um réttindi og skyldur starfsmanna ríkisins, nr. 70/1996.

Ákvæði um öryggisvottun fyrirtækja vegna útflutningshagsmuna eru sett skv. 14. gr. laga um eftirlit með þjónustu og hlutum sem geta haft hernaðarlega þýðingu, nr. 58/2010.

Reglugerðin öðlast þegar gildi. Gildandi öryggisvottanir og/eða -viðurkenningar halda gildi sínu í samræmi við gildistíma þeirra eða þar til ný öryggisvottun og/eða -viðurkenning hefur verið gefin út.

Utanríkisráðuneytinu, 28. október 2012.

Össur Skarphéðinsson.

Einar Gunnarsson.

B-deild – Útgáfud.: 14. nóvember 2012