Väljaandja:	Vabariigi Valitsus
Akti liik:	määrus
Teksti liik:	terviktekst
Redaktsiooni jõustumise kp:	01.07.2017
Redaktsiooni kehtivuse lõpp:	
Avaldamismärge:	RT I, 28.06.2017, 56

Riigisaladuse ja salastatud välisteabe kaitse kord

Vastu võetud 20.12.2007 nr 262
RT I 2007, 73, 449
jõustumine 01.01.2008

Muudetud järgmiste aktidega

Vastuvõtmine	Avaldamine	Jõustumine
11.12.2008	RT I 2008, 55, 312	01.01.2009
17.12.2009	RT I 2009, 65, 448	01.01.2010
06.01.2011	RT I, 14.01.2011, 6	17.01.2011
15.03.2012	RT I, 19.03.2012, 1	22.03.2012
14.08.2014	RT I, 19.08.2014, 17	22.08.2014, määruses asendatud läbivalt sõna „kaitsevägi” sõnaga „Kaitsevägi” vastavas käändes.
23.09.2016	RT I, 27.09.2016, 5	30.09.2016
20.10.2016	RT I, 26.10.2016, 2	29.10.2016
17.11.2016	RT I, 22.11.2016, 7	01.01.2017
25.05.2017	RT I, 31.05.2017, 7	03.06.2017
22.06.2017	RT I, 28.06.2017, 40	01.07.2017, tekstis asendatud sõna „Teabeamet” sõnaga „Välisluureamet” vastavas käändes.

Määrus kehtestatakse «Riigisaladuse ja salastatud välisteabe seaduse» § 11 lõike 1, § 13 lõike 5, § 14 lõike 4, § 15 lõigete 4 ja 5, § 20 lõigete 4 ja 6, § 27 lõike 13, § 31 lõike 5, § 36 lõike 3, § 39 lõike 1, § 41 lõike 6, § 42 lõike 4, § 46 lõike 4 ja § 51 lõike 6 alusel.

1. peatükk
ÜLDSÄTTED

§ 1. Määruse reguleerimisala

Käesoleva määrusega kehtestatakse riigisaladuse ja salastatud välisteabe kaitse kord ning riigisaladuseks oleva teabe alaliigid, teabe alaliigi salastamistase ja -tähtaeg.

§ 2. Mõisted

Käesolevas määruses kasutatakse mõisteid järgmises tähenduses:
1) salastatud teave – riigisaladus või salastatud välisteave;
2) töötlev üksus – salastatud teavet töötlev asutus, põhiseaduslik institutsioon või juriidiline isik või töötlemisloa alusel salastatud teavet töötlev füüsiline isik;
3) administratiivala – töötleva üksuse kasutuses olev selge välispiiriga ala, millele sisenenud kõik isikud ja sõidukid tuvastatakse ning millel on lubatud piiratud tasemel salastatud teabe töötlemine;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
4) avalik ruum – ala, mis ei ole turva- ega administratiivala;
5) salastamisandmete parandamine – õigusliku aluseta riigisaladusena töödeldava teabe salastatuse kustutamine; valel tasemel, valel õiguslikul alusel või vale tähtajaga salastatud riigisaladuse taseme, õigusliku aluse või tähtaja muutmine;
6) avatud hoiuala – turvaala, kus ei pea kasutama seifi ega lukustatavat kappi või sahtlit;
7) kuller – isik, kes edastab salastatud teabekandjat.

§ 2[1]. Riigi julgeoleku volitatud esindaja

Riigi julgeoleku volitatud esindaja on Välisluureameti struktuuriüksus.
[RT I, 22.11.2016, 7- jõust. 01.01.2017]

§ 3. Ministeeriumi kantsleri volitamine

Minister võib ministeeriumi kantslerit volitada tegema kõiki toiminguid ja otsuseid, mida minister saab käesoleva korra kohaselt teha asutuse juhina.

2. peatükk
RIIGISALADUSE ALALIIGID

§ 4. Välissuhete riigisaladuse alaliigid

(1) Välissuhtlemisasutuse loodud rahvusvahelisi suhteid käsitleva sellise teabe ja välissuhtlemisasutuse loodud sellise teabe osas, mille avalikuks tulek kahjustaks oluliselt Eesti Vabariigi välissuhtlemist, on riigisaladuseks:
1) välissuhtlemisasutuse töötaja või esindaja rahvusvahelisel kohtumisel saadud või kohtumist käsitlev teave, mille avalikustamine võib oluliselt kahjustada riigi julgeolekut. Selline teave salastatakse salajasel tasemel 50 aastaks;
2) välissuhtlemisasutuse töötaja või esindaja rahvusvahelisel kohtumisel saadud või kohtumist käsitlev teave, mille avalikustamine võib kahjustada riigi julgeolekut või oluliselt kahjustada välissuhtlemist. Selline teave salastatakse piiratud tasemel kohtumisel osalenud poolte kokkulepitud tähtpäeva või sündmuse saabumiseni, kuid mitte kauemaks kui 50 aastaks;
3) välissuhtlemisasutuse loodud teave rahvusvaheliste läbirääkimiste või kohtumiste ettevalmistamise ja läbiviimise kohta, mille avalikuks tulek enne läbirääkimiste või kohtumise toimumist võib kahjustada riigi julgeolekut või oluliselt kahjustada välissuhtlemist. Selline teave salastatakse piiratud tasemel kuni kohtumise toimumiseni või 50 aastaks, kui teabe avalikustamine pärast kohtumist või kohtumise ärajäämise korral kahjustaks riigi julgeolekut või oluliselt kahjustaks välissuhtlemist;
4) rahvusvaheliste visiitide või tseremooniate (selles punktis edaspidi *üritus*) ettevalmistamist või läbiviimist kajastav teave, välja arvatud juhul, kui selle avalikuks tulek ei kahjusta riigi julgeolekut ega kahjusta oluliselt välissuhtlemist. Selline teave salastatakse piiratud tasemel kuni ürituse toimumiseni või 50 aastaks, kui teabe avalikustamine pärast üritust või ürituse ärajäämise korral kahjustaks riigi julgeolekut või oluliselt kahjustaks välissuhtlemist;
5) rahvusvahelisel kohtumisel saadud või kohtumist kajastav välissuhtlemisasutuse loodud teave, mida kaitstakse avalikuks tuleku eest rahvusvaheliste tavade kohaselt või mille kaitsmises on kohtumisel või muul üritusel osalejate vahel kokku lepitud. Selline teave salastatakse osalejate kokkuleppel või rahvusvahelise tava kohaselt määratud tasemel ja tähtajaks, kuid mitte kõrgemal kui salajasel tasemel ja mitte kauemaks kui 50 aastaks;
6) välissuhtlemisasutuse loodud teave, mis käsitleb rahvusvahelisi suhteid, välisriiki või rahvusvahelist institutsiooni või nende esindajat, kui teabe sisu, selle edastamise viisi või allika avalikustamine kahjustaks riigi julgeolekut või kahjustaks oluliselt välissuhtlemist. Selline teave salastatakse piiratud tasemel 50 aastaks.

(2) Strateegilise kauba sisseveo, väljaveo, transiidi, sõjalise kaubaga seotud teenuse väljaveo ja strateegilise kauba lõppkasutuse kohta Välisministeeriumi juures tegutseva strateegilise kauba komisjoni kogutud ja koostatud teabe osas on riigisaladuseks:
1) strateegilise kauba komisjoni ülesannete täitmiseks kogutud teave strateegilise kauba sisseveo, väljaveo, transiidi, sõjalise kaubaga seotud teenuse väljaveo ja strateegilise kauba lõppkasutuse kohta, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 30 aastaks;
2) strateegilise kauba komisjoni ülesannete täitmiseks strateegilise kauba sisseveo, väljaveo, transiidi, sõjalise kaubaga seotud teenuse väljaveo ja strateegilise kauba lõppkasutuse kohta koostatud teave, milles analüüsitakse strateegilise kauba levikut ja sellega seotud ohtu julgeolekule. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
3) strateegilise kauba kontrolli rahvusvahelisele kontrollsüsteemile – Wassenaari kokkuleppe osalistele – ja Euroopa Liidu tavarelvastuse töögrupile edastatav teave strateegilise kauba komisjoni poolt sõjalise kauba, välja arvatud massihävitusrelvadega seotud materjalid, rajatised ja seadmed, sisseveo- või väljaveolitsentsi, transiidiloa või lõppkasutuse järelevalve dokumendi väljastamisest keeldumise kohta; samuti teave sellist keeldumist arutanud strateegilise kauba komisjoni koosolekul käsitletu kohta. See teave salastatakse piiratud tasemel 10 aastaks;
4) strateegilise kauba kontrolli rahvusvahelistele kontrollsüsteemidele – tuumatarnijate grupile ja Austraalia grupile – edastatav strateegilise kauba komisjoni koostatud teave massihävitusrelvadega seotud materjalide, rajatiste ja seadmete sisseveo- või väljaveolitsentsi, transiidiloa või lõppkasutuse järelevalve dokumendi väljastamisest keeldumise kohta; samuti teave sellist keeldumist arutanud strateegilise kauba komisjoni koosolekul käsitletu kohta. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks.

§ 5. Riigikaitse riigisaladuse alaliigid

(1) Sõjalise riigikaitse ettevalmistamist, juhtimist ja tegevust käsitleva teabe osas on riigisaladuseks:
1) Kaitseväe sõjaaja üksuste koosseisu kuuluvate struktuuriüksuste ja reservüksuste (välja arvatud grupi, Kaitseväe Ühendatud Õppeasutuste ja NATO küberkaitsekoostöö keskuse Eesti kontingendi)

tüüpkoosseisutabelid ning Kaitseväe sõjaaja üksuste koosseisu kuuluvate struktuuriüksuste ja reservüksuste tüüpvarustustabelid. See teave salastatakse piiratud tasemel 10 aastaks või kuni sõjaseisukorra ajal mobilisatsiooni väljakuulutamiseni;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

1[1]) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

2) [kehtetu -RT I 2008, 55, 312- jõust. 01.01.2009]

3) Kaitseväe sõjalise riigikaitse riigi ulatuses operatiivplaneerimist ja operatiivjuhtimist kajastav teave. See teave salastatakse salajasel tasemel 50 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

3[1]) Kaitseväe sõjalise riigikaitse riigi territoriaalsel jaotusel põhinevat operatiivplaneerimist ja operatiivjuhtimist kajastav teave. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

4) Kaitseväe väeliigi, väejuhatuse, brigaadi ja Kaitseväe korralduse seaduse § 37 lõike 1 punktides 1, 2 ja 5 ning lõikes 2 nimetatud viisil teavet koguva kaitseväeluure ülesannet või erioperatsioonide korraldamise ülesannet täitva üksuse operatiivplaneerimist ja operatiivjuhtimist kajastav teave. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

5) Kaitseväe struktuuriüksuse ja reservüksuse operatiivplaneerimist ja operatiivjuhtimist kajastav teave, mida ei salastata punktide 3–4 alusel. See teave salastatakse piiratud tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

6) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

7) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

8) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

9) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

10) Kaitseväe sõjalisel operatsioonil osalemist kajastav teave, mille avalikuks tulek võib ohustada operatsiooni korraldamist või kahjustada osaleva üksuse julgeolekut. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks sõjalise operatsiooni lõppemisest arvates;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

11) Kaitseväe sõjaaja üksuste ja reservüksuste tervikstruktuur, nende koguarv ja nende koosseisus olevate ametikohtade arv. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

12) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

13) teave sõjaaja raadiosageduste kohta. See teave salastatakse salajasel tasemel 50 aastaks;

14) Kaitseväe mereseiresüsteemide andmeedastusseadmete parameetrid ja tegevusvõime. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;

15) Kaitseväe sõjalaevade magnet- ja akustiliste väljade mõõtmise tulemused. See teave salastatakse salajasel tasemel 10 aastaks;

16) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

17) Kaitseväe jõu kasutamise kord, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

18) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

19) Kaitseväe erioperatsioonide korraldamise ülesannet täitva struktuuriüksuse ja allüksuse struktuuri ja koosseisu (välja arvatud struktuuriüksuste ülemate ametikohad), ülesandeid ja teenistujate tööülesandeid, ametikohtade komplekteerimist ja täituvust, eelarve kulude liigendust, eelarve täitmise aruandlust, eelarve planeerimist ja investeeringuid kajastav teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 25 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

20) teave Kaitseväe erioperatsioone korraldava struktuuriüksuse ülesande täitmisel kasutatavate meetodite ja vahendite kohta, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 25 aastaks.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(2) Mobilisatsiooni ettevalmistamist ja läbiviimist käsitleva teabe osas on riigisaladuseks:

1) mobilisatsiooniregistrisse kantud andmed kogumis. See teave salastatakse salajasel tasemel 30 aastaks;

2) Kaitseväe sõjaaja üksuste koosseisu kuuluvate struktuuriüksuste täidetud ametikohtade andmed kogumis. See teave salastatakse salajasel tasemel 30 aastaks;

3) Kaitseväe sõjaaja üksuste koosseisu kuuluva ühe struktuuriüksuse või reservüksuse täidetud ametikohtade andmed kogumis. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks;

4) Kaitseväe sõjaaja üksuste koosseisu kuuluvate struktuuriüksuste olemasoleva varustuse andmed kogumis. See teave salastatakse salajasel tasemel 30 aastaks;

5) Kaitseväe sõjaaja üksuste koosseisu kuuluva ühe struktuuriüksuse või reservüksuse olemasoleva varustuse andmed kogumis. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks;

6) Kaitseväe sõjaaja üksuste koosseisu kuuluvate struktuuriüksuste lahinguvalmidust kajastavad andmed. See teave salastatakse salajasel tasemel 30 aastaks;

7) Kaitseväe sõjaaja üksuste koosseisu kuuluva ühe struktuuriüksuse või reservüksuse lahinguvalmidust kajastavad andmed. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks.

[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(3) Mobilisatsiooni korraldamiseks vajalikku varu käsitleva teabe osas on riigisaladuseks teave mobilisatsiooni korraldamiseks vajaliku varu ja vahendite üldkoguste kohta. See teave salastatakse salajasel tasemel 10 aastaks.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(4) Kaitseväe ja Kaitseliidu sõjaväerelvi ja lahingumoona käsitleva teabe osas on riigisaladuseks:
1) Kaitseväe ja Kaitseliidu sõjaväerelvade ja lahingumoona koondandmeid ja -jaotust kajastav teave, välja arvatud teave, mille avaldamine on kohustuslik välislepingu alusel. See teave salastatakse salajasel tasemel 20 aastaks;
2) [kehtetu -RT I 2008, 55, 312- jõust. 01.01.2009]
3) mereväe relvasüsteemide taktikalised andmed, välja arvatud mereväebaasi relvasüsteemide taktikalised andmed. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(5) Kaitseväe radariteabe ja seiresüsteemidelt kogutud teabe osas on riigisaladuseks:
1) [kehtetu -RT I, 14.01.2011, 6- jõust. 17.01.2011]
2) õhuväe õhuseireradari võime parameetrid, mille avalikuks tulek võib kahjustada õhuseiret. See teave salastatakse piiratud tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
3) õhuväe õhuseiresüsteemi koondparameetrid ja radarite võime parameetrid, mille avalikuks tulek võib kahjustada õhuseiret. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
4) radari elektroonilise sõjapidamise meetmete ja vahendite tehniline kirjeldus. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
5) radari elektroonilise sõjapidamise võime testi tulemused. See teave salastatakse salajasel tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
6) radari kasutatavad töörežiimid, filtreeritud alad ja sihtmärgi kriteeriumid. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
7) radari tegevusseisund ja hooldusajad üldise kaitsevalmiduse ajal. See teave salastatakse piiratud tasemel üheks aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
8) radari tegevusseisund ja hooldusajad kõrgendatud kaitsevalmiduse, sõjaseisukorra, erakorralise seisukorra ja mobilisatsiooni ajal. See teave salastatakse salajasel tasemel üheks aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
9) radari ja seiresüsteemi kõrgendatud kaitsevalmiduse, sõjaseisukorra, erakorralise seisukorra ja mobilisatsiooni ajaks planeeritud asukoht täpsusega üle ühe sekundi. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
10) teave õhukaitsesüsteemi koodnimetuse kohta. See teave salastatakse piiratud tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
11) radari hoolduse ja analüüsi tulemused. See teave salastatakse piiratud tasemel viieks aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
12) sekundaarradari identifitseerimiskriteeriumide tuvastamist võimaldavad krüptoseadmed ja krüptovõtmed. See teave salastatakse salajasel tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
13) õhuseiresüsteemi poolt kogutud ja töödeldud terviklik radariteave. See teave salastatakse konfidentsiaalsel tasemel viieks aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
14) teave õhukaitsesüsteemi paiknemise kohta täpsusega üle ühe sekundi ning vastutus- ja jälgimisala kohta. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
15) teave õhukaitsesüsteemi tegevusseisundi kohta üldise kaitsevalmiduse ajal. See teave salastatakse piiratud tasemel üheks aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
16) teave õhukaitsesüsteemi tegevusseisundi kohta kõrgendatud kaitsevalmiduse, sõjaseisukorra, erakorralise seisukorra ja mobilisatsiooni ajal. See teave salastatakse salajasel tasemel üheks aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
17) mereseirevahenditega kogutud ja analüüsitud teave. See teave salastatakse salajasel tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
18) teave mereseiresüsteemi merepildi tuvastus- ja analüüsivõime kohta. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
19) teave konkreetsetes kasutustingimustes laevadele paigutatud mereseiresüsteemide seadistuse kohta. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(6) Riigikaitselisi leiutisi ja uuringuid ning nende tulemusi käsitleva teabe osas on riigisaladuseks riigikaitselisi leiutisi ja uuringuid käsitlev teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel või madalamal tasemel kuni 30 aastaks.

[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(7) Kaitseväeluurega tegeleva Kaitseväe struktuuriüksuse kogutud ja sünteesitud teabe osas on riigisaladuseks:
1) sideluure vahenditega kogutud teave või selle põhjal sünteesitud teave, mille põhjal on võimalik tuvastada kogumisviis. See teave salastatakse täiesti salajasel tasemel 50 aastaks;
2) elektroonilise luure vahenditega kogutud teave või selle põhjal sünteesitud teave. See teave salastatakse salajasel tasemel 30 aastaks;
3) varjatud jälgimise teel kogutud teave või selle põhjal sünteesitud teave. See teave salastatakse salajasel tasemel 30 aastaks;
3^1) inimluure kaudu kogutud teave või selle põhjal sünteesitud teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 50 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
3^2) julgeolekuluure teave või selle põhjal sünteesitud teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 50 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
4) punktides 3–3^2nimetatud teave, kui selle avaldamisega kaasneks oht inimese elule või tervisele. See teave salastatakse täiesti salajasel tasemel 50 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
5) teave, mis kajastab riigi julgeolekut ähvardava ohu allikaid. See teave salastatakse konfidentsiaalsel tasemel 15 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
6) teave, mis kajastab välisriike, rahvusvahelisi organisatsioone, välismaiseid sõjalisi tegureid ja tegevust. See teave salastatakse piiratud tasemel 15 aastaks;
7) kaitseväeluuret teostava Kaitseväe struktuuriüksuse poolt koostatud ohuhinnangut käsitlev teave. See teave salastatakse salajasel tasemel 50 aastaks;
8) kaitseväeluuret teostava Kaitseväe struktuuriüksuse poolt julgeolekuasutuste korraldatud luure- ja vastuluureoperatsioonide käigus kogutud teave või selle alusel sünteesitud teave. See teave salastatakse salajasel tasemel 30 aastaks;
9) välisriigi, rahvusvahelise organisatsiooni, rahvusvahelise kokkuleppega loodud institutsiooni või julgeolekuasutuste teave, mille lähteandmed on salastatud kõrgemal tasemel või pikemaks ajaks, kui on sätestatud punktides 5 ja 6. See teave salastatakse lähteandmete salastatuse kõrgeimat taset ja pikimat salastamise tähtaega sätestava riigisaladuse alaliigi alusel;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
10) piltluure kaudu kogutud teave või selle põhjal sünteesitud teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 15 aastaks.
[RT I 2008, 55, 312- jõust. 01.01.2009]

(8) Kaitseväe korralduse seaduse § 37 lõike 1 punktides 1, 2 ja 5 ning lõikes 2 nimetatud viisil teavet koguva Kaitseväe struktuuriüksuse koosseisu, ülesandeid ja eelarve jaotust käsitleva teabe osas on riigisaladuseks:
[RT I, 19.08.2014, 17- jõust. 22.08.2014]
1) struktuuriüksuse või allüksuste struktuurid, koosseisu käsitlev teave ja ametikohtade jaotus ning paiknemine struktuuriüksustes eraldiseisvalt ja andmekoguna, välja arvatud struktuuriüksuste ülemate ametikohad ja teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 25 aastaks;
2) struktuuriüksuse või allüksuse ülesanded ja nende teenistujate tööülesanded ning tööülesandeid käsitlev teave, välja arvatud teave, mille avalikustamine ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 25 aastaks;
3) struktuuriüksuse või allüksuse teenistujate koondandmed, samuti andmed Kaitseväe luure värbamisstatistika ja ametikohtade komplekteerimise ning täituvuse osas. See teave salastatakse salajasel tasemel 25 aastaks;
4) struktuuriüksuse või allüksuse eelarve kulude liigendus, eelarve täitmise aruandlus, eelarve planeering ja investeeringud, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 25 aastaks.
[RT I 2008, 55, 312- jõust. 01.01.2009]

(9) [Kehtetu -RT I 2008, 55, 312- jõust. 01.01.2009]

(10) «Kaitseväe korralduse seaduse» § 37 lõike 1 punktides 1 ja 2 ning lõikes 2 nimetatud viisil teavet koguva kaitseväeluuret teostava Kaitseväe struktuuriüksusepoolt teabe kogumist kajastava teabe, kaasa arvatud kogumiseks kasutatavate meetodite, vahendite ja jälgitavaid objekte käsitleva teabe osas on riigisaladuseks:
1) struktuuriüksuse poolt teabe varjatud kogumisel kasutatavad meetodid, taktika ja vahendid ning neid kajastav teave. See teave salastatakse salajasel tasemel 50 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
2) signaalluure ja muude tehniliste luurevahendite võimeid käsitlev teave. See teave salastatakse salajasel tasemel 50 aastaks;
3) signaalluure ja muude tehniliste luurevahendite võimet tagavad süsteemid või vahendid. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks;
4) teabe kogumise alustamiseks ja lõpetamiseks tehtud otsuseid käsitlev teave. See teave salastatakse salajasel tasemel 50 aastaks;

5) andmed Kaitseväe poolt Kaitseväe korralduse seaduse alusel salajast koostööd tegema kaasatud isiku kohta. See teave salastatakse salajasel tasemel 50 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
6) andmed, millest nähtub Kaitseväe poolt teeseldud juriidilise isiku, tema struktuuriüksuse, organi, äriühingu filiaali või variisiku seotus Kaitseväega. See teave salastatakse salajasel tasemel 50 aastaks.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(11) Kaitseväeluurealast rahvusvahelist koostööd käsitleva teabe osas on riigisaladuseks:
1) teave välissuhtluse kohta, kui see ei sisalda käesoleva lõike punktides 2–4 nimetatud teavet või ei kahjusta riigi julgeolekut. See teave salastatakse piiratud tasemel 30 aastaks;
2) teave koostöö kohta välisriigi ja rahvusvahelise organisatsiooniga, kui see ei sisalda käesoleva lõike punktides 3 ja 4 nimetatud teavet. See teave salastatakse konfidentsiaalsel tasemel 50 aastaks, kui ei ole kokku lepitud teisiti. Teavet ei salastata, kui see on õiguspäraselt avalikustatud;
3) rahvusvahelise koostöö käigus varjatult kogutud teave ja selle teabe vahetamist kajastav teave. See teave salastatakse salajasel tasemel 50 aastaks, kui ei ole kokku lepitud teisiti;
4) koos välisriigi politsei- või julgeolekuasutusega varjatult kogutud luure- ja vastuluure alane teave ja selle kogumist kajastav teave. See teave salastatakse täiesti salajasel tasemel 50 aastaks, kui ei ole kokku lepitud teisiti.
[RT I 2008, 55, 312- jõust. 01.01.2009]

(12) Kaitseväe ja Kaitseliidu militaargeograafia valdkonda käsitleva teabe osas on riigisaladuseks:
1) mõõtkavas 1:50 000 kaitsejõudude ruumiandmebaas, kolmemõõtmelised maastikumudelid, töödeldud kaugseireandmed. See teave salastatakse piiratud tasemel 10 aastaks;
[RT I 2008, 55, 312- jõust. 01.01.2009]
2) Kaitseväe koostatud strateegilise ja taktikalise tasandi maastikuanalüüsid Eesti riigi territooriumi kohta, riigikaitseliste objektide geokoordineeritud plaanid ja riigikaitseliste objektide kolmemõõtmelised geograafilised mudelid. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
3) Kaitseväe poolt välisriigi territooriumi kohta koostatud strateegilise ja taktikalise tasandi maastikuanalüüsid, riigikaitseliste objektide koordineeritud plaanid, töödeldud kaugseireandmed ja kolmemõõtmelised mudelid. See teave salastatakse salajasel tasemel 30 aastaks.

§ 6. Korrakaitse riigisaladuse alaliigid

(1) Jälitusasutuste poolt jälitustegevuse käigus kogutud teabe ning teabe kogumisel kasutatud meetodeid, taktikat ja vahendeid käsitleva teabe osas on riigisaladuseks:
1) tunnistajakaitse teostamiseks jälitustegevuse käigus kogutud teave. See teave salastatakse salajasel tasemel 25 aastaks;
2) jälitusasutuse poolt jälitustoiminguga kogutud teave. See teave salastatakse piiratud tasemel 25 aastaks. Sellise teabe salastatus kustub selles ulatuses, mis on kantud kriminaaltoimikusse või mida tutvustatakse isikule, kelle suhtes jälitustoiming tehti, või isikule, kelle perekonna- või eraelu puutumatust jälitustoiminguga riivati;
3) jälitusasutuse poolt jälitustegevuses salajasele koostööle kaasatud isikult saadud teave. See teave salastatakse piiratud tasemel 50 aastaks;
4) Politsei- ja Piirivalveameti poolt koostatud organiseeritud ja muu raske kuritegevuse ohuhinnangutes ning ülevaadetes kajastuv jälitustegevuse käigus kogutud teave. See teave salastatakse piiratud tasemel 50 aastaks;
[RT I 2009, 65, 448- jõust. 01.01.2010]
5) jälitustegevuses kasutatavaid meetodeid, taktikat ja vahendeid kajastav teave, välja arvatud teave, mis on tuletatav õiguspäraselt avaldatud jälitustoiminguga kogutud teabest. See teave salastatakse piiratud tasemel 25 aastaks;
6) teave jälitusasutuse poolt jälitustegevuses salajasele koostööle kaasatud isiku tasu, hüvitise ja neilt tasutud maksude ning neid kajastavate dokumentide kohta. See teave salastatakse piiratud tasemel 25 aastaks;
7) andmed jälitusasutuse poolt teeseldud isiku või organi kohta, mis võivad paljastada tema seotust jälitusasutusega. See teave salastatakse piiratud tasemel 25 aastaks.

(2) Jälitusasutuste poolt jälitustegevuses salajasele koostööle kaasatud isiku ja variisiku kohta käivate andmete osas on riigisaladuseks andmed jälitusasutuse poolt jälitustegevuses salajasele koostööle kaasatud isiku ja variisiku identiteedi kohta. See teave salastatakse piiratud tasemel 75 aastaks. Salastatus kustub, kui isiku surmast on möödunud 20 aastat, kuid mitte varem kui 50 aastat teabe salastamisest arvates.

(3) Andmed jälitusasutuste politseiagendi kohta on riigisaladus. See teave salastatakse piiratud tasemel 75 aastaks. Sellise teabe salastatus kustub selles ulatuses, mis on kantud kriminaaltoimikusse. Kriminaaltoimikusse kandmata teabe salastatus kustub, kui isiku surmast on möödunud 20 aastat, kuid mitte varem kui 50 aastat teabe salastamisest arvates.

(4) Politsei- ja Piirivalveameti tunnistajakaitse struktuuriüksuse struktuuri, koosseisu ja ülesandeid kajastava teabe osas on riigisaladuseks Politsei- ja Piirivalveameti tunnistajakaitse struktuuriüksuse struktuuri, koosseisu ja selle ametikohtadel töötavaid isikuid ning nende ülesandeid kajastav teave Politsei- ja Piirivalveameti juhi käskkirjaga määratud ulatuses. See teave salastatakse salajasel tasemel 50 aastaks.
[RT I 2009, 65, 448- jõust. 01.01.2010]

(5) Politsei- ja Piirivalveameti tunnistajakaitse struktuuriüksuse kasutuses olevat vara ja eelarve jaotust kajastava teabe osas on riigisaladuseks:

1) teave Politsei- ja Piirivalveameti tunnistajakaitse struktuuriüksuse poolt kasutatavate transpordivahendite kohta, kui selle avalikuks tulek ohustaks tunnistajakaitse kohaldamist või tunnistajakaitse struktuuriüksuse või kaitse alla võetud isiku turvalisust. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
2) teave Politsei- ja Piirivalveameti tunnistajakaitse struktuuriüksuse poolt kasutatava vara kohta, kui selle avalikuks tulek ohustaks tunnistajakaitse kohaldamist või tunnistajakaitse struktuuriüksuse või kaitse alla võetud isiku turvalisust. See teave salastatakse salajasel tasemel 25 aastaks;
3) Politsei- ja Piirivalveameti tunnistajakaitse struktuuriüksuse eelarve kulude liigendus ja eelarve täitmise aruandlus. See teave salastatakse salajasel tasemel 25 aastaks.
[RT I 2009, 65, 448- jõust. 01.01.2010]

(6) Tunnistajakaitse kaitseabinõusid käsitleva teabe osas on riigisaladuseks:
1) tunnistajakaitse kaitseabinõude kohaldamise meetodeid ja taktikaid käsitlev teave. See teave salastatakse salajasel tasemel 50 aastaks;
2) „Tunnistajakaitse seaduse“ § 14 lõike 6 ja § 19 alusel määrusega kehtestatav tunnistajakaitse kaitselepingu vorm ning kaitsetoimiku pidamise ja säilitamise kord. See teave salastatakse piiratud tasemel 25 aastaks.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

(7) Konkreetse isiku suhtes tunnistajakaitse kaitseabinõude kohaldamist kajastava teabe osas on riigisaladuseks:
1) konkreetse isiku suhtes tunnistajakaitse kaitseabinõude kohaldamist kajastav teave, välja arvatud teave, mis kajastab üksnes tunnistajakaitse alla võtmise fakti. See teave salastatakse täiesti salajasel tasemel 75 aastaks. Salastatus kustub, kui tunnistajakaitse all olnud isiku surmast on möödunud 20 aastat, kuid mitte vähem kui 50 aastat teabe salastamisest arvates;
2) Politsei- ja Piirivalveameti tunnistajakaitse struktuuriüksuse eelarve kulude liigendus ja eelarve täitmise aruandlus, kui selles kajastuvad konkreetse isiku suhtes rakendatavad kaitseabinõud. See teave salastatakse täiesti salajasel tasemel 75 aastaks. Salastatus kustub, kui tunnistajakaitse all olnud isiku surmast on möödunud 20 aastat, kuid mitte vähem kui 50 aastat dokumendi salastamisest arvates.
[RT I 2009, 65, 448- jõust. 01.01.2010]

(8) Riiklikus kriisireguleerimisplaanis erakorralise seisukorra ja sõjaseisukorra ajal tegutsemist käsitleva teabe osas on riigisaladuseks riiklikus kriisireguleerimisplaanis erakorralise seisukorra ja sõjaseisukorra ajal tegutsemist käsitlev teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse täiesti salajasel tasemel 50 aastaks. Salastatus kustub teabe avalikul kasutamisel erakorralise seisukorra või sõjaseisukorra ajal.

(9) [Kehtetu -RT I, 27.09.2016, 5- jõust. 30.09.2016]

(10) [Kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

§ 7. Julgeolekuasutuste riigisaladuse alaliigid

(1) Julgeolekuasutuste rahvusvahelist koostööd kajastava teabe osas on riigisaladuseks:
1) julgeolekuasutuse koostatud teave julgeolekualase välissuhtluse kohta, kui see ei sisalda käesoleva lõike punktides 2–4 nimetatud teavet. See teave salastatakse piiratud tasemel 30 aastaks;
2) julgeolekuasutuse julgeolekualast koostööd välisriigi või rahvusvahelise organisatsiooniga kajastav teave, kui see ei hõlma käesoleva lõike punktides 3 ja 4 nimetatud teavet. See teave salastatakse konfidentsiaalsel tasemel 50 aastaks, kui ei ole kokku lepitud teisiti. Seda teavet ei salastata, kui see on õiguspäraselt avalikustatud;
3) julgeolekuasutuse rahvusvahelise koostöö käigus edastatav varjatult kogutud teave ja selle teabe vahetamist kajastav teave. See teave salastatakse salajasel tasemel 50 aastaks, kui ei ole kokku lepitud teisiti;
4) julgeolekuasutuse poolt koos välisriigi politsei- või julgeolekuasutusega varjatult kogutud teave ja selle kogumist kajastav või selle käigus vahetatav teave. See teave salastatakse täiesti salajasel tasemel 50 aastaks, kui ei ole kokku lepitud teisiti.

(2) Julgeolekuasutuse kasutatava vara ja julgeolekuasutuse eelarve jaotust kajastava teabe osas on riigisaladuseks:
1) teave julgeolekuasutuse kasutatava vara kohta, kui selle avalikuks tulek ohustaks julgeolekuasutuse ülesande täitmist või julgeolekuasutuse turvalisust. See teave salastatakse konfidentsiaalsel tasemel kuni vara kasutamise või hoone või rajatise valdamise lõppemiseni, kuid mitte kauemaks kui 25 aastaks;
2) teave teabe varjatult kogumiseks kasutatavate tehniliste vahendite kohta, kui selle avalikuks tulek ohustaks julgeolekuasutuse ülesande täitmist. See teave salastatakse salajasel tasemel 50 aastaks;
3) julgeolekuasutuse eelarve kulude liigendus ja eelarve täitmise aruandlus. See teave salastatakse salajasel tasemel 25 aastaks.

(3) Hädaolukorra lahendamisel julgeolekuasutuse tegevust kajastava teabe osas on riigisaladuseks hädaolukorra lahendamisel julgeolekuasutuse tegevust kajastav teave, sealhulgas kasutatavad meetodid ja taktika ning hädaolukorra lahendamisel osalevate ametnike tegevusjuhised. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks. Salastatus kustub teabe avalikul kasutamisel hädaolukorras.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(4) Julgeolekuasutuse ülesannete täitmisel varjatult kogutud teabe ja selle kogumist kajastava teabe osas on riigisaladuseks:
1) «Julgeolekuasutuste seaduse» alusel varjatult kogutud ja kogutav teave ning töökorraldused selle teabe kogumiseks. See teave salastatakse salajasel tasemel 50 aastaks. Salastatus kustub, kui julgeolekuasutuse ülesannete täitmiseks on julgeolekuasutuse peadirektori otsusel vajalik teabe avalik kasutamine. Käesolevat punkti ei kohaldata elektroonilise side ettevõtja või isikuandmete töötleja seadmes automaatselt talletatavate logide kohta;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
2) punktis 1 nimetatud teave, kui selle avaldamisega kaasneks oht inimese elule või tervisele või täiesti salajasel tasemel salastatud teabe kaitstusele. See teave salastatakse täiesti salajasel tasemel 50 aastaks;
3) punktis 1 nimetatud teabe kogumise meetodid ja taktika. See teave salastatakse salajasel tasemel 50 aastaks;
4) signaalluure meetodeid ja allikaid kajastav teave. See teave salastatakse täiesti salajasel tasemel 50 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
5) «Julgeolekuasutuste seaduse» alusel teabe varjatud kogumise toimingute loetelusid sisaldav aruandlus, milles ei kajastu täiesti salajasel tasemel salastatav teave. See teave salastatakse salajasel tasemel 25 aastaks;
6) Vabariigi Valitsuse ja Vabariigi Valitsuse julgeolekukomisjoni poolt julgeolekuasutusele teabe kogumiseks antavad ülesanded. See teave salastatakse salajasel tasemel 25 aastaks;
7) Kaitsepolitseiameti poolt «Julgeolekuasutuste seaduse» alusel teabe varjatud kogumise käigus laekunud teave toimepandud või ettevalmistatavate kuritegude kohta, mis ei ole Kaitsepolitseiameti uurimisalluvuses, juhul kui selles ei avaldu teabe allikad, kogumise taktika või käesoleva lõike punktides 2–6 nimetatud teave. See teave salastatakse piiratud tasemel 25 aastaks.

(5) Julgeolekuasutuse ülesannete täitmisel analüüsitud ja sünteesitud teabe osas on riigisaladuseks:
1) julgeolekuasutuse ülesannete täitmisel analüüsitud ja sünteesitud teave, mis kajastab välisriike, välismaiseid tegureid või tegevust. See teave salastatakse piiratud tasemel 15 aastaks;
2) julgeolekuasutuse ülesannete täitmisel analüüsitud ja sünteesitud teave, mis kajastab riigisiseseid või välismaiseid ohuallikaid. See teave salastatakse konfidentsiaalsel tasemel 15 aastaks;
3) julgeolekuasutuse poolt koostatud ohuhinnangud, välja arvatud käesoleva lõike punktis 3^1nimetatud ohuhinnangud. See teave salastatakse salajasel tasemel 50 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
3^1) julgeolekuasutuse poolt koostatud ohuhinnangud julgeolekuasutuse uurimisalluvuses olevate kuritegude kohta. See teave salastatakse piiratud tasemel 25 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
4) ürituse, objekti või isiku julgestamise eesmärgil julgeolekuasutuse poolt koostatud ohuhinnang. See teave salastatakse piiratud tasemel 15 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
5) julgeolekuasutuse analüüsitud või sünteesitud teave, mille lähteandmed on salastatud kõrgemal tasemel või pikemaks ajaks, kui on sätestatud punktides 1–4, salastatakse lähteandmete kõrgeimat taset ja pikimat tähtaega sätestava riigisaladuse alaliigi alusel;
6) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
7) valitsusasutuse ettepanek või ülesanne julgeolekuasutusele analüüsida või sünteesida punktides 1–3 nimetatud teavet või koostada punktides 3^1ja 4 nimetatud ohuhinnang, välja arvatud teave, mille avalikustamine ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse ettepanekust või ülesandest lähtudes vastavalt punktides 1–4 määratud tasemel ja tähtajaks.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(5^1) Lõike 5 alusel ei salastata teavet, mis koostatakse eesmärgiga avalikkuse teavitamise teel ennetada ohtu või riigi huvide kahjustamist või teavitada avalikkust julgeolekuasutuse tegevusest. Samuti ei salastata teabe seda osa, mis kantakse kriminaaltoimikusse.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(6) Julgeolekuasutuse struktuuriüksusi, koosseisu ja nende ülesandeid kajastava teabe osas on riigisaladuseks:
1) julgeolekuasutuse struktuur, välja arvatud struktuuriüksused, mis avaldatakse vastava julgeolekuasutuse põhimääruses. See teave salastatakse salajasel tasemel 25 aastaks;
2) julgeolekuasutuse struktuuriüksuste ja teenistujate ülesanded, välja arvatud teave, mille avalikustamine ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 25 aastaks;
3) julgeolekuasutuse teenistujate koondandmed ja üksnes teabe varjatud kogumisega seonduvaid tööülesandeid täitvate teenistujate koosseis. See teave salastatakse salajasel tasemel 25 aastaks;
4) [kehtetu -RT I, 14.01.2011, 6- jõust. 17.01.2011]
5) julgeolekuasutuse poolt tehnilise julgeoleku kontrolli käigus antud hinnangud ja tehtud analüüsid. See teave salastatakse piiratud tasemel 25 aastaks.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(7) Andmed julgeolekuasutuse poolt salajasele koostööle kaasatud isiku ja salajase koosseisulise julgeolekuasutuse ametniku või töötaja kohta, välja arvatud § 6 lõikes 2 nimetatud teave, on riigisaladus. See teave salastatakse täiesti salajasel tasemel 75 aastaks. Salastatus kustub, kui isiku surmast on möödunud 20 aastat, kuid mitte varem kui 50 aastat teabe salastamisest arvates.
[RT I, 28.06.2017, 40- jõust. 01.07.2017]

(8) Andmed isiku kohta, kes «Eestit okupeerinud riikide julgeolekuorganite või relvajõudude luure- või vastuluureorganite teenistuses olnud või nendega koostööd teinud isikute arvelevõtmise ja avalikustamise

korra seaduse» § 5 lõike 2 punktis 1 sätestatud korras on Kaitsepolitseiametile esitanud isikliku ülestunnistuse julgeoleku- või luureorgani teenistuses olemise või sellega koostöö tegemise kohta, välja arvatud juhul, kui julgeoleku- või luureorgani teenistuses olnud või sellega koostööd teinud isik on eelnimetatud teenistuse või koostööga seonduvalt pannud toime õigusrikkumise, mis Eesti Vabariigis kehtiva õiguse kohaselt on karistatav esimese astme kuriteona, või on toime pannud kuriteo inimsuse vastu või sõjakuriteo ning õigusrikkumise või kuriteo toimepanemine selle isiku poolt on kohtulikult tõendatud jõustunud kohtulahendiga või kui julgeoleku- või luureorgani teenistuses oli või tegi sellega koostööd Vabariigi President või Riigikogu, Vabariigi Valitsuse või Riigikohtu liige, on riigisaladus. See teave salastatakse salajasel tasemel 50 aastaks. Salastatus kustub, kui isiku surmast on möödunud 20 aastat, kuid mitte varem kui 50 aastat teabe salastamisest arvates.

(9) Julgeolekuasutuste tegevuse koordineerimist, nende koostööd Kaitseväega ja Vabariigi Valitsuse julgeolekukomisjoni tööd käsitleva teabe osas on riigisaladuseks:
1) Riigikantseleis julgeolekuasutuste töö koordineerimisega ja Vabariigi Valitsuse julgeolekukomisjoni töö korraldamisega seotud ametnike või Siseministeeriumis ja Kaitseministeeriumis julgeolekuasutuste töö suunamise ja koordineerimisega seotud ametnike ja töötajate koostatud teave julgeolekualase välissuhtluse kohta, kui see ei sisalda punktis 2 nimetatud teavet. See teave salastatakse piiratud tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
2) Riigikantseleis julgeolekuasutuste tööd koordineeriva ja Vabariigi Valitsuse julgeolekukomisjoni tööd korraldava struktuuriüksuse või Siseministeeriumis ja Kaitseministeeriumis julgeolekuasutuste tööd suunava ja koordineeriva struktuuriüksuse julgeolekualast koostööd välisriigi või rahvusvahelise organisatsiooniga kajastav teave. See teave salastatakse konfidentsiaalsel tasemel 50 aastaks, kui ei ole kokku lepitud teisiti. Seda teavet ei salastata, kui see on õiguspäraselt avalikustatud;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
3) teave Vabariigi Valitsuse julgeolekukomisjoni ja selle alakomisjoni istungitel käsitletavate teemade kohta, välja arvatud teave, mida Vabariigi Valitsuse julgeolekukomisjoni otsusega ei käsitata riigisaladusena või mis avalikustatakse eesmärgiga ennetada ohtu või riigi huvide kahjustamist. See teave salastatakse piiratud tasemel 25 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
4) Riigikantseleis julgeolekuasutuste tööd koordineeriva ja Vabariigi Valitsuse julgeolekukomisjoni tööd korraldava struktuuriüksuse ja teenistujate või Siseministeeriumis ja Kaitseministeeriumis julgeolekuasutuste tööd suunava ja koordineeriva struktuuriüksuse ja teenistujate ülesanded, välja arvatud teave, mille avalikustamine ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 25 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
5) Riigikantseleis julgeolekuasutuste tööd koordineeriva ja Vabariigi Valitsuse julgeolekukomisjoni tööd korraldava struktuuriüksuse poolt koostatud ohuhinnangud ja riigi julgeolekuteabe hanke ja analüüsi kava. See teave salastatakse salajasel tasemel 50 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
6) Riigikantseleis julgeolekuasutuste tööd koordineeriva ja Vabariigi Valitsuse julgeolekukomisjoni tööd korraldava struktuuriüksuse või Siseministeeriumis ja Kaitseministeeriumis julgeolekuasutuste tööd suunava ja koordineeriva struktuuriüksuse poolt julgeolekuteabe alusel analüüsitud ning koostatud teave. See teave salastatakse salajasel tasemel 50 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
6^1) Siseministeeriumi ja Kaitseministeeriumi koostatud julgeolekuasutuse tegevuse suunamist ja koordineerimist kajastav teave, välja arvatud teave, mille avalikustamine ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 25 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
6^2) julgeolekuasutuse teenistuslikku järelevalvet või auditeerimist kajastav teave, välja arvatud teave, mille avalikustamine ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 25 aastaks.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
7) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

(9^1) Teave, mille lähteandmed on salastatud kõrgemal tasemel või pikemaks tähtajaks, kui on sätestatud lõike 9 punktides 3 ja 6–6^2, salastatakse lähteandmete salastatuse kõrgeimat taset ja pikimat salastamise tähtaega sätestava riigisaladuse alaliigi alusel.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(10) Julgeolekuasutuse poolt teeseldud isikute ja organite ning kasutatavate variandmete kohta käiva teabe osas on riigisaladuseks teave, millest nähtub teeseldud isikute ja organite või kasutatavate variandmete seotus julgeolekuasutusega. See teave salastatakse salajasel tasemel 50 aastaks.

(11) Julgeolekuasutuse dokumendiregistris sisalduv teave on riigisaladus. See teave salastatakse salajasel tasemel 25 aastaks või kõrgemal tasemel ja pikemaks tähtajaks, kui register sisaldab vastava salastatuse taseme ja tähtajaga teavet.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

§ 8. Infrastruktuuri ja teabe kaitse riigisaladuse alaliigid

(1) Vabariigi Presidendi Kantselei, Riigikantselei, julgeolekuasutuse, Kaitseministeeriumi, Kaitseväe, Kaitseliidu, Kaitseressursside Ameti, Riigi Infosüsteemi Ameti, Eesti Panga, Siseministeeriumi, Politsei- ja Piirivalveameti ja Välisministeeriumi, sealhulgas välisesinduste, ning nende valitsusasutuste hallatavate riigiasutuste valve-, häire-, side- ja infosüsteeme käsitleva teabe osas on riigisaladuseks:
[RT I, 22.11.2016, 7- jõust. 01.01.2017]
1) käesoleva lõike sissejuhatavas osas nimetatud asutuse valduses oleva ehitise või maa-ala elektroonilise läbipääsu- või valvesüsteemi koondteave ühe ehitise või maa-ala või selle tervikuna käsitatava osa ulatuses, mis sisaldab andmeid süsteemi moodustavate seadmete, sealhulgas keskseadmete asukoha, tüübi, nendevaheliste ühenduste ja teiste tehniliste näitajate kohta või andmeid valvealade või -tsoonide kohta või süsteemi üldist kirjeldust, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
2) käesoleva lõike sissejuhatavas osas nimetatud asutuse valduses oleva ehitise või maa-ala elektroonilise läbipääsu- või valvesüsteemi toimimist ja efektiivsust kajastavad analüüsid ja hinnangud, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
3) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
4) käesoleva lõike sissejuhatavas osas nimetatud asutuse valduses oleva ehitise või maa-ala elektroonilise läbipääsu- või valvesüsteemi koondteave ühe ehitise või maa-ala või selle tervikuna käsitatava osa ulatuses, mis sisaldab andmeid süsteemi kuuluvate lõppseadmete (andurid, kaamerad või muud seadmed) asukoha ja tüübi ning nendest moodustatavate valvealade ja -tsoonide või süsteemi seadistuse kohta, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
5) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
6) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
7) käesoleva lõike sissejuhatavas osas nimetatud asutuse valduses oleva ehitise või maa-ala elektroonilises läbipääsu- või valvesüsteemis töödeldav teave kogumis, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
8) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
9) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
10) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
11) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
12) käesoleva lõike sissejuhatavas osas nimetatud asutuse valduses oleva ehitise või maa-ala automaatse tulekahjusignalisatsioonisüsteemi koondteave ühe ehitise või selle tervikuna käsitatava osa ulatuses, mis sisaldab andmeid süsteemi moodustavate seadmete asukoha, tüübi, nendevaheliste ühenduste ja teiste tehniliste näitajate kohta või süsteemi üldist kirjeldust, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
13) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
14) käesoleva lõike sissejuhatavas osas nimetatud asutuse valduses oleva ehitise või maa-ala füüsiliste julgeolekumeetmete analüüsid ja hinnangud, mis kajastavad julgeolekumeetmete toimimist ja efektiivsust, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
15) teave Kaitseväes signaalluureks, õhuseireks, mereseireks, objektide turbeks ja valveks ning riigi sõjaliseks kaitsmiseks ja selle juhtimiseks püsivalt kasutatavate raadiosageduste kohta. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
16) Kaitseministeeriumi, Kaitseväe, Kaitseliidu, Kaitseressursside Ameti ja teiste Kaitseministeeriumi valitsemisalas olevate teabevaldajate riigi sõjaliseks kaitsmiseks ja selle juhtimiseks kasutatavate sidevõrkude ja töötlussüsteemide koondteave, sealhulgas iga sidevõrgu ja töötlussüsteemi ülesehituse koondteave ja turvameetmeid käsitlev teave. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
17) [kehtetu -RT I, 19.08.2014, 17- jõust. 22.08.2014]
18) Kaitseministeeriumi, Kaitseväe, Kaitseliidu, Kaitseressursside Ameti ja teiste Kaitseministeeriumi valitsemisalas olevate teabevaldajate asutusesiseseks kasutamiseks mõeldud teabe töötlemiseks kasutatavate sidevõrkude ja töötlussüsteemide, milles ei töödelda salastatud teavet, tehnilisi andmeid ja turvameetmeid kajastav teave. See teave salastatakse piiratud tasemel kuni sidevõrgu või töötlussüsteemi või selle osa kasutamise lõppemiseni, kuid mitte kauemaks kui 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
19) [kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]
20) teave õhuväe õhuseire sidesüsteemis kasutatava krüptoseadme kirjelduse kohta. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
21) teave õhuväe õhuseire sidesüsteemis kasutatava võtmeta krüptoseadme kohta. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
22) teave õhuväe õhuseire sidesüsteemis kasutatava võtmega krüptoseadme kohta. See teave salastatakse salajasel tasemel 10 aastaks;

23) teave õhuväe õhuseire sidesüsteemis kasutatavate sidelinkide skeemide kohta. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
24) teave õhuseiresüsteemide andmeedastusseadmete parameetrite ja tegevusvõime kohta. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
25) käesoleva lõike sissejuhatavas osas nimetatud asutuse teave kaabelduse kohta ühe ehitise või maa-ala või selle tervikuna käsitatava osa ulatuses, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 30 aastaks või kuni võrgu võõrandamiseni või kasutamise lõppemiseni;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
25^1) käesoleva lõike sissejuhatavas osas nimetatud asutuse teave konfidentsiaalsel ja kõrgemal tasemel salastatud teabe töötlussüsteemi kaabelduse kohta ühe ehitise või maa-ala või selle tervikuna käsitatava osa ulatuses. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks või kuni võrgu võõrandamiseni või kasutamise lõppemiseni;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
26) Välisluureameti poolt eriside korraldamiseks ning kontrollimiseks kasutatavaid meetodeid ja vahendeid kajastav teave. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
27) välispiiride valvamiseks mõeldud Politsei- ja Piirivalveameti seire- ja valvesüsteemide tehniline teave ja tööparameetrid, mis ei ole avalikest allikatest kättesaadav ja mille avalikuks tulek kahjustab sisejulgeoleku tagamist. See teave salastatakse piiratud tasemel 10 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
28) välispiiride valvamiseks mõeldud Politsei- ja Piirivalveameti seire- ja valvesüsteemide ülesehituse ja tehniliste parameetrite kohta käiv koondteave, mis sisaldab süsteemide üldist kirjeldust või andmeid süsteemi kuuluvate seadmete täpsete tehniliste näitajate kohta. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
29) välispiiride valvamiseks mõeldud Politsei- ja Piirivalveameti seire- ja valvesüsteemide katvuspiirkondi kajastavate testide tulemused. See teave salastatakse piiratud tasemel 10 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
30) välispiiride valvamiseks mõeldud andmeside detailset tehnilist ülesehitust või turbemeetodeid käsitlev teave kogumis. See teave salastatakse piiratud tasemel 10 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
31) operatiivraadioside detailset ülesehitust või turbemeetodeid käsitlev teave kogumis, välja arvatud võrgu ülesehituse koondnumbrid. See teave salastatakse piiratud tasemel 20 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
32) Riigi Infosüsteemi Ameti küberturvalisuse riskianalüüsid, seireteave ning järelevalvetoimingute käigus infosüsteemide kriitilise haavatavuse kohta kogutud teave ulatuses, milles need sisaldavad tehnilist teavet põhiseaduslike institutsioonide, valitsusasutuste, nende hallatavate asutuste, elutähtsa teenuse osutajate ning Eestis paiknevate ja Eesti poolt tagatava julgeolekuga rahvusvaheliste organisatsioonide infosüsteemide kriitilise haavatavuse kohta, ja mille teatavaks saamine kõrvalistele isikutele tekitab küberturvalisuse intsidendi tekke ohu nendes valdkondades, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 10 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
33) välispiiride valvamiseks mõeldud Politsei- ja Piirivalveameti seire- ja valvesüsteemide juhtimissüsteemi ülesehitust kajastav teave kogumis. See teave salastatakse piiratud tasemel 20 aastaks.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(1^1) Riigikaitseseaduse tähenduses riigikaitseobjektide, välja arvatud käesoleva paragrahvi lõikes 1 nimetatud asutuste valduses olevate riigikaitseobjektide ja avaliku korra tagamiseks oluliste riigikaitseobjektide valve- ja häiresüsteeme ning kaitsemeetmeid käsitleva teabe osas on riigisaladuseks:
1) avaliku võimu organi kasutuses oleva või elutähtsa teenuse osutamisega või sisejulgeoleku tagamisega seotud riigikaitseobjekti riskianalüüsis ja turvaplaanis riigikaitseobjekti elektroonilist läbipääsu- või valvesüsteemi ning riigikaitseobjekti füüsilise kaitse miinimummeetmeid ja lisaturvameetmeid käsitlev koondteave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 10 aastaks;
2) riigikaitseobjekti, selle täpset paiknemist ning seoseid teiste riigikaitseobjektidega käsitlev teave, mis ohustab kaitsemeetmete rakendamist, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 20 aastaks.
[RT I, 27.09.2016, 5- jõust. 30.09.2016]

(2) Riigisaladuse ja salastatud välisteabe töötlussüsteeme käsitleva teabe osas on riigisaladuseks:
1) valdkonna eest vastutava ministri määrusega kehtestatavad krüptomaterjalide ning nende töötlemise ja kaitse nõuded. See teave salastatakse piiratud tasemel 30 aastaks;
[RT I, 19.08.2014, 17- jõust. 22.08.2014]
2) valdkonna eest vastutava ministri määrusega kehtestatavad kiirgusturbe tagamise nõuded. See teave salastatakse piiratud tasemel 30 aastaks;
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

3) töötlussüsteemi seadmete kiirgusturbe mõõtmise tulemused, kui neid ei ole avaldanud tootja ise, ning töötlussüsteemi asukoha ruumide kiirgusturbe mõõtmise tulemused. See teave salastatakse konfidentsiaalsel tasemel 25 aastaks;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
3[1]) töötleva üksuse krüptomaterjali registreerimist puudutavad andmed, sealhulgas registreerimiseks kasutatava dokumendiregistri kanded. See teave salastatakse piiratud tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
4) Välisluureametis krüptomaterjali registreerimist puudutavad andmed kogumina. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
5) salastatud teabe valdajale spetsiaalselt salastatud teabe töötlemiseks loodud tarkvara lähtekood. See teave salastatakse piiratud tasemel 30 aastaks;
6) piiratud tasemel salastatud teavet töötleva töötlussüsteemi tehnilisi andmeid ja turvameetmeid kajastav teave. See teave salastatakse piiratud tasemel 30 aastaks;
7) konfidentsiaalse või kõrgema taseme salastatud teabe töötlussüsteemis teabe töötlemise tingimused ja kasutajate ülesannete jagunemine salastatud teabe töötlemisel. See teave salastatakse piiratud tasemel 30 aastaks;
8) konfidentsiaalsel tasemel salastatud teavet töötleva töötlussüsteemi tehnilisi andmeid ja turvameetmeid kajastav teave. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
9) salajasel tasemel salastatud teavet töötleva töötlussüsteemi tehnilisi andmeid ja turvameetmeid kajastav teave. See teave salastatakse salajasel tasemel 50 aastaks;
10) täiesti salajasel tasemel salastatud teavet töötleva töötlussüsteemi tehnilisi andmeid ja turvameetmeid kajastav teave. See teave salastatakse täiesti salajasel tasemel 50 aastaks.

(3) Lõike 1 punktis 18 ning lõike 2 punktides 6 ja 8–10 nimetatud töötlussüsteemi tehnilisi andmeid ja turvameetmeid kajastav teave on teave, millest nähtuvad:
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
1) [kehtetu -RT I, 14.01.2011, 6- jõust. 17.01.2011]
2) töötlussüsteemi tehniline kirjeldus;
2[1]) töötlussüsteemi toimimist ja efektiivsust kajastavad analüüsid ja hinnangud;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
3) töötlussüsteemi võrguskeem;
4) tehniline teave töötlussüsteemi teise infotöötlussüsteemiga ühendamise kohta ning teave rakendatavate turvameetmete kohta;
5) töötlussüsteemis elektrooniliste krüptovõtmete haldamise tarkvara seadistus;
6) õigusaktis sätestatud elektroonilise teabeturbe nõude täitmata jätmise kompenseerimiseks rakendatav turvameede;
7) töötlussüsteemi riskianalüüsi tulemused;
8) töötlussüsteemi jääkriskide hinnangud;
9) töötlussüsteemi haavatavuse analüüsi tulemused.

(4) Kaitseväe korralduse seaduse § 37 lõike 1 punktides 1, 2 ja 5 ning lõikes 2 nimetatud viisil teavet koguva kaitseväeluure ülesannet täitva Kaitseväe struktuuriüksuse kasutuses olevaid hooneid ja rajatisi käsitleva teabe osas on riigisaladuseks teave struktuuriüksuse erivajadusteks kohandatud hoonete ja ruumide kohta, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse konfidentsiaalsel tasemel 50 aastaks või hoone või rajatise valduse lõppemiseni.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

(5) Kaitseväe ja Kaitseliidu relva- ja lahingumoonaladusid käsitleva teabe osas on riigisaladuseks:
1) teave relva- või lahingumoonalao turvalisuse tagamise erinõuete kohta, välja arvatud valvesüsteemide kohta kehtestatud nõuded. See teave salastatakse piiratud tasemel 10 aastaks või kuni relva- või laskemoonalao valduse lõppemiseni;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
2) Kaitseväe ja Kaitseliidu sõjaväerelvade ja lahingumoona ladude andmed kogumis. See teave salastatakse piiratud tasemel 20 aastaks.

(6) Teabevaldaja salastatud teabekandjate evakueerimist käsitleva teabe osas on riigisaladuseks konfidentsiaalsel või kõrgemal tasemel salastatud teavet sisaldavate teabekandjate evakueerimist käsitlev teave. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks.

(7) Teabevaldaja turvaala valve- ja häiresüsteeme käsitleva teabe osas on riigisaladuseks:
1) teave, mis sisaldab andmeid salastatud teabe valdaja turvaala elektroonilise läbipääsu- või valvesüsteemi moodustavate seadmete asukoha, tüübi, nendevaheliste ühenduste ja teiste tehniliste näitajate kohta või andmeid valvealade või -tsoonide kohta või süsteemi üldist kirjeldust. See teave salastatakse konfidentsiaalsel tasemel kuni ala turvaalana kasutamise lõpetamiseni, kuid mitte kauemaks kui 30 aastaks;
2) salastatud teabe valdaja turvaala elektroonilise läbipääsu- või valvesüsteemi toimimist ja efektiivsust kajastavad analüüsid ja hinnangud. See teave salastatakse konfidentsiaalsel tasemel kuni ala turvaalana kasutamise lõpetamiseni, kuid mitte kauemaks kui 30 aastaks;
3) salastatud teabe valdaja turvaala füüsiliste julgeolekumeetmete analüüsid ja hinnangud, mis kajastavad julgeolekumeetmete toimimist ja efektiivsust. See teave salastatakse konfidentsiaalsel tasemel kuni ala turvaalana kasutamise lõpetamiseni, kuid mitte kauemaks kui 30 aastaks.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(7[1]) Kui teabevaldaja turvaala elektrooniline läbipääsu- või valvesüsteem on suurema süsteemi osa, salastatakse vaid turvaalale paigaldatud seadmeid kajastav teave.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(8) Eesti Panga sularaha vedu käsitleva teabe osas on riigisaladuseks:
1) teave Eesti Panga riikidevahelise veo aja ja veetava summa kohta. See teave salastatakse piiratud tasemel kuni veo lõppemiseni;
2) teave Eesti Panga riikidevahelise veo marsruudi ja julgestamise kohta. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(9) Katkematu side korraldamist käsitleva teabe osas on riigisaladuseks katkematu side korraldamise kord ja nõuded katkematule sidele ning katkematu sidega varustatud objektide ja nende sidevahendite loetelu kogumis. See teave salastatakse piiratud tasemel 25 aastaks.
[RT I, 19.03.2012, 1- jõust. 22.03.2012]

3. peatükk
RIIGISALADUSE SALASTATUSE KUSTUTAMINE, SALASTAMISALUSE, -TASEME JA -TÄHTAJA MUUTMINE

1. jagu
Riigisaladuse salastatuse ennetähtaegne kustutamine

§ 9. Salastatuse ennetähtaegse kustutamise taotluse esitamine

(1) Asutus või põhiseaduslik institutsioon, kellel puudub pädevus kustutada enda loodud riigisaladuse salastatust enne tähtaja möödumist, esitab «Riigisaladuse ja salastatud välisteabe seaduse» § 13 lõikes 4 sätestatud juhul taotluse riigisaladuse salastatuse ennetähtaegseks kustutamiseks Vabariigi Valitsusele ministri kaudu, kelle valitsemisalasse ta kuulub. Kui asutus või põhiseaduslik institutsioon ei asu ühegi ministeeriumi valitsemisalas, esitab ta taotluse Vabariigi Valitsusele Siseministeeriumi kaudu.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

(2) Taotluses märgitakse salastatuse ennetähtaegse kustutamise vajaduse põhjendused, millisele asutusele või põhiseaduslikule institutsioonile on see teave edastatud ja kas teave oleks pärast kustutamist asutusesiseseks kasutamiseks mõeldud teave. Taotlusele lisatakse selle kohta esitatud vastuväited. «Riigisaladuse ja salastatud välisteabe seaduse» § 13 lõikes 2 nimetatud teabe korral lisatakse taotlusele ka füüsilise isiku kirjalik nõusolek.

(3) Ministril on õigus suunata taotlus Vabariigi Valitsuse julgeolekukomisjonile arvamuse andmiseks.

§ 10. Taotluse kohta vastuväidete esitamine

(1) Paragrahvi 9 lõikes 1 nimetatud asutus või põhiseaduslik institutsioon peab enne salastatuse kustutamise taotlemist teavitama taotluse esitamise kavatsusest kõiki asutusi ja põhiseaduslikke institutsioone, kellele seda riigisaladust sisaldav teabekandja on edastatud, ja andma neile vastuväidete esitamiseks vähemalt ühekuulise tähtaja. Samuti teavitatakse vajaduse korral asutust ja põhiseaduslikku institutsiooni, kelle ülesandeid see teave võib puudutada.

(2) Salastatuse ennetähtaegse kustutamise kavatsuse teates märgitakse salastatuse ennetähtaegse kustutamise vajaduse põhjendused ja kas teave oleks pärast salastatuse kustutamist asutusesiseseks kasutamiseks mõeldud teave.

(3) Teate saanud asutus või põhiseaduslik institutsioon esitab riigisaladuse salastatuse ennetähtaegsele kustutamisele vastuväited hiljemalt käesoleva paragrahvi lõike 1 alusel antud tähtaja jooksul.

(4) Minister kaalub taotluse Vabariigi Valitsusele esitamisel taotlusele esitatud vastuväiteid.

§ 11. Kustutamiseks pädeva asutuse poolt kustutamise kavatsusest teavitamine

(1) Asutus või põhiseaduslik institutsioon, kes on pädev kustutama enda loodud riigisaladuse salastatust enne tähtaja möödumist, peab kustutamise kavatsusest teavitama kõiki asutusi ja põhiseaduslikke institutsioone, kellele seda riigisaladust sisaldav teabekandja on edastatud, ja andma neile vastamiseks vähemalt ühekuulise tähtaja. Samuti teavitatakse vajaduse korral asutust ja põhiseaduslikku institutsiooni, kelle ülesandeid see teave võib puudutada.

(2) Kustutamise kavatsuse teates märgitakse salastatuse ennetähtaegse kustutamise põhjendused, kavandatav kustutamise kuupäev ja selgitus, kas teave oleks edaspidi asutusesiseseks kasutamiseks mõeldud teave.

(3) Teate saanud asutus või põhiseaduslik institutsioon esitab salastatuse ennetähtaegse kustutamise kohta vastuväited käesoleva paragrahvi lõike 1 alusel antud tähtaja jooksul.

(4) Lõikes 1 nimetatud asutuse või põhiseadusliku institutsiooni juht kaalub salastatuse ennetähtaegse kustutamise otsustamisel asutuste ja põhiseaduslike institutsioonide vastuväiteid.

§ 12. «Riigisaladuse ja salastatud välisteabe seaduse» § 35 lõikes 3 nimetatud asutuse ja põhiseadusliku institutsiooni teavitamine salastatuse ennetähtaegsest kustutamisest

Kui §-des 10 ja 11 nimetatud teate saanud asutus või põhiseaduslik institutsioon on kõnealuse riigisaladuse edastanud «Riigisaladuse ja salastatud välisteabe seaduse» § 35 lõikes 3 nimetatud asutusele või põhiseaduslikule institutsioonile, teavitab ta seda asutust või põhiseaduslikku institutsiooni riigisaladuse ennetähtaegse kustutamise kavatsuse teate saamisest. Sel viisil teavitatud asutusel ja põhiseaduslikul institutsioonil on õigus esitada oma vastuväited samas korras, salastatuse ennetähtaegse kustutamise taotluse esitamist või ennetähtaegset kustutamist kavatseva asutuse või põhiseadusliku institutsiooni antud tähtaja jooksul.

§ 13. Ennetähtaegsest kustutamisest teavitamine

(1) Kui asutus või põhiseaduslik institutsioon on kustutanud enda loodud riigisaladuse salastatuse enne tähtaja möödumist, teavitab ta sellest viivitamata kõiki töötlevaid üksusi, kes seda riigisaladust sisaldavat teabekandjat valdavad.

(2) Kui Vabariigi Valitsus kustutab riigisaladuse salastatuse enne tähtaja möödumist ministri taotluse või ministri edastatud taotluse alusel, teavitab minister salastatuse kustutamisest viivitamata kõiki asutusi ja põhiseaduslikke institutsioone, kellele seda riigisaladust sisaldav teabekandja on edastatud.

(3) Asutus või põhiseaduslik institutsioon, kes on edastanud salastatud teabekandja, mille salastatus on kustutatud, «Riigisaladuse ja salastatud välisteabe seaduse» § 35 lõikes 3 nimetatud asutusele või põhiseaduslikule institutsioonile, teavitab salastatuse kustutamisest viivitamata ka seda asutust või põhiseaduslikku institutsiooni.

2. jagu
Riigisaladuse salastamistähtaja pikendamine

§ 14. Salastamistähtaja pikendamise taotlus

(1) Asutus või põhiseaduslik institutsioon, kellel puudub pädevus pikendada enda loodud riigisaladuse salastamistähtaega, esitab taotluse salastamistähtaja pikendamiseks Vabariigi Valitsusele ministri kaudu, kelle valitsemisalasse ta kuulub. Kui asutus või põhiseaduslik institutsioon ei asu ühegi ministeeriumi valitsemisalas, esitab ta taotluse Vabariigi Valitsusele Siseministeeriumi kaudu.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

(2) Riigisaladuseks oleva teabe salastamistähtaja pikendamise taotlus esitatakse Vabariigi Valitsusele võimaluse korral vähemalt kolm kuud enne salastamistähtaja lõppu.

(3) Taotluses märgitakse salastamistähtaja pikendamise vajaduse põhjendused ja millisele asutusele või põhiseaduslikule institutsioonile on see teave edastatud. Taotlusele lisatakse selle kohta esitatud vastuväited.

(4) Ministril on õigus suunata taotlus Vabariigi Valitsuse julgeolekukomisjonile arvamuse andmiseks.

§ 15. Salastamistähtaja pikendamise kohta vastuväidete esitamine

(1) Paragrahvi 14 lõikes 1 nimetatud asutus või põhiseaduslik institutsioon peab enne salastamistähtaja pikendamise taotlemist teavitama taotluse esitamise kavatsusest kõiki asutusi ja põhiseaduslikke institutsioone, kellele seda riigisaladust sisaldav teabekandja on edastatud, ja andma neile vastamiseks vähemalt ühekuulise tähtaja.

(2) Pikendamise kavatsuse teates märgitakse salastamistähtaja pikendamise põhjendused.

(3) Teate saanud asutus või põhiseaduslik institutsioon esitab riigisaladuse salastamistähtaja pikendamisele vastuväited käesoleva paragrahvi lõike 1 alusel antud tähtaja jooksul.

(4) Minister kaalub taotluse Vabariigi Valitsusele esitamisel taotlusele esitatud vastuväiteid.

§ 16. Salastamistähtaja pikendamisest teavitamine

(1) Kui asutus või põhiseaduslik institutsioon on pikendanud enda loodud riigisaladuse salastamistähtaega, teavitab ta sellest viivitamata kõiki töötlevaid üksusi, kes seda riigisaladust sisaldavat teabekandjat valdavad.

(2) Kui Vabariigi Valitsus on pikendanud riigisaladuse salastamistähtaega ministri taotluse või ministri poolt edastatud taotluse alusel, teavitab minister salastatuse pikendamisest viivitamata kõiki asutusi ja põhiseaduslikke institutsioone, kellele seda riigisaladust sisaldav teabekandja on edastatud.

(3) Asutus või põhiseaduslik institutsioon, kes on edastanud salastatud teabekandja, mille salastamistähtaega on pikendatud, «Riigisaladuse ja salastatud välisteabe seaduse» § 35 lõikes 3 nimetatud asutusele või põhiseaduslikule institutsioonile, teavitab salastatuse pikendamisest viivitamata ka seda asutust või põhiseaduslikku institutsiooni.

3. jagu
Salastamisandmete parandamine

§ 17. Salastamisandmete parandamise taotluse esitamine

(1) Asutus või põhiseaduslik institutsioon, kelle töötajal või teenistujal puudub pädevus salastamisandmete parandamiseks, esitab «Riigisaladuse ja salastatud välisteabe seaduse» § 15 lõikes 1 sätestatud juhul taotluse salastamisandmete parandamiseks vastavalt Vabariigi Valitsusele või Siseministeeriumile selle ministri kaudu, kelle valitsemisalasse ta kuulub. Töötlemisloaga isik esitab taotluse riigisaladuse töötlemise loa saamist toetanud asutuse kaudu.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

(2) Taotluses märgitakse salastamisandmete parandamise põhjendused ja selgitus, kas teave oleks edaspidi juurdepääsupiiranguta avalik või asutusesiseseks kasutamiseks mõeldud teave või millisel alusel või millise tähtajaga salastatud teave ning millistele asutustele ja põhiseaduslikele institutsioonidele on see teave edastatud. Taotlusele lisatakse selle kohta esitatud vastuväited.

(3) Ministril on õigus suunata taotlus Vabariigi Valitsuse julgeolekukomisjonile arvamuse andmiseks.

§ 18. Salastamisandmete parandamise taotluse esitamise kavatsusest teavitamine

(1) Enne salastamisandmete parandamise taotluse esitamist peab taotluse esitamise kavatsusest teavitama kõiki asutusi ja põhiseaduslikke institutsioone, kellele seda riigisaladust sisaldav teabekandja on edastatud, ja andma neile vastamiseks vähemalt ühekuulise tähtaja.

(2) Salastamisandmete parandamise teates märgitakse salastamisandmete parandamise põhjendused ja selgitus, kas teave oleks edaspidi juurdepääsupiiranguta avalik või asutusesiseseks kasutamiseks mõeldud teave või millisel alusel või millise tähtajaga salastatud teave.

(3) Teate saanud asutus või põhiseaduslik institutsioon esitab riigisaladuse salastamisandmete parandamisele vastuväited hiljemalt käesoleva paragrahvi lõike 1 alusel antud tähtaja jooksul.

(4) Salastamisandmete parandamine otsustatakse taotluse ja sellele esitatud vastuväidete alusel.

§ 19. Enda loodud riigisaladuse salastamisandmete parandamise kavatsusest teavitamine

(1) Töötlev üksus peab enne enda loodud riigisaladuse salastamisandmete parandamist sellest kavatsusest teavitama kõiki asutusi ja põhiseaduslikke institutsioone, kellele seda riigisaladust sisaldav teabekandja on edastatud, andes vastamiseks vähemalt ühekuulise tähtaja.

(2) Teates märgitakse salastamisandmete parandamise põhjendused ja selgitus, kas teave oleks edaspidi juurdepääsupiiranguta avalik või asutusesiseseks kasutamiseks mõeldud teave või millisel alusel või millise tähtajaga salastatud teave.

(3) Teate saanud asutus või põhiseaduslik institutsioon esitab vastuväited salastamisandmete parandamisele käesoleva paragrahvi lõike 1 alusel antud tähtaja jooksul.

(4) Lõikes 1 nimetatud töötlev üksus kaalub salastamisandmete parandamise otsustamisel teiste asutuste ja põhiseaduslike institutsioonide vastuväiteid.
[RT I 2008, 55, 312- jõust. 01.01.2009]

§ 20. «Riigisaladuse ja salastatud välisteabe seaduse» § 35 lõikes 3 nimetatud asutuse ja põhiseadusliku institutsiooni teavitamine salastamisandmete parandamise kavatsusest

Kui teate saanud asutus või põhiseaduslik institutsioon on riigisaladuse edastanud «Riigisaladuse ja salastatud välisteabe seaduse» § 35 lõikes 3 nimetatud asutusele või institutsioonile, teavitab ta seda asutust või põhiseaduslikku institutsiooni riigisaladuse salastamisandmete parandamise kavatsuse teate saamisest. Sel viisil teavitatud asutusel või põhiseaduslikul institutsioonil on õigus esitada oma vastuväited samas korras parandamise kavatsuse teate saanud asutuste ja põhiseaduslike institutsioonidega, salastamisandmete parandamisele vastuväidete esitamiseks antud tähtaja jooksul.

§ 21. Salastamisandmete parandamisest teavitamine

(1) Kui töötlev üksus parandab salastamisandmeid, teavitab ta sellest viivitamata kõiki töötlevaid üksusi, kellele seda riigisaladust sisaldav teabekandja on edastatud.

(2) Kui salastamisandmete parandamise on otsustanud Vabariigi Valitsus taotluse alusel, teavitab taotluse esitanud ministeerium sellest kõiki töötlevaid üksusi, kellele seda riigisaladust sisaldav teabekandja on edastatud.

(3) Kui salastamisandmeid parandatakse väärteo- või kohtuotsusega, teavitab Kaitsepolitseiamet kõiki töötlevaid üksusi, kellele seda riigisaladust sisaldav teabekandja on edastatud.

(4) Töötlev üksus, kes on edastanud salastatud teabekandja, mille salastamisandmed on parandatud, «Riigisaladuse ja salastatud välisteabe seaduse» § 35 lõikes 3 nimetatud asutusele või põhiseaduslikule institutsioonile, samuti ministeerium, kes on edastanud konfidentsiaalsel või madalamal tasemel salastatud riigisaladuse oma allasutusele, teavitab salastamisandmete muutmisest viivitamata seda asutust või põhiseaduslikku institutsiooni.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

4. peatükk
SALASTATUD TEABE KAITSE KORRALDAMISE NÕUDED

§ 22. Riigisaladust valdava asutuse, põhiseadusliku institutsiooni ja juriidilise isiku riigisaladuse kaitse juhendile esitatavad nõuded

(1) Riigisaladust valdava asutuse, põhiseadusliku institutsiooni ja juriidilise isiku riigisaladuse kaitse juhendis reguleeritakse järgmisi küsimusi, arvestades töötleva üksuse eripära:
1) väljastpoolt saabuvate ja väljapoole saadetavate salastatud teabekandjate vastuvõtmise ja edastamise kord;
2) salastatud teabekandjate registreerimise kord;
3) seifi võtme ja ligipääsukoodi hoiustamise kord;
4) juurdepääsuloa ja juurdepääsusertifikaadi käitlemise kord;
5) salastamisandmete parandamise kord;
6) salastatud koosolekute pidamise kord;
7) turvaala asukoht;
8) turvaala valve, turvaalale pääsemise, sellel liikumise ja sealt lahkumise kord;
9) salastatud teabe kaitse plaan ohuolukorras;
10) teavitamine isikust, kes püüab mis tahes viisil saavutada ebaseaduslikku juurdepääsu salastatud teabele, ning «Riigisaladuse ja salastatud välisteabe seaduse» või selle alusel antud õigusakti nõuete rikkumisest;
11) loend kõikide asutuses, põhiseaduslikus institutsioonis ja juriidilises isikus kehtivate selliste kordade, juhendite ja muude eeskirjade kohta, mis reguleerivad riigisaladuse töötlemist;
12) salastatud teabekandja hävitamise meetod ja kord;
13) administratiivala ulatus;
14) relva ning tehnilise vahendi ja muu eseme, mida saab kasutada tehnilise vahendina pealtkuulamiseks või salvestamiseks, turvaalale viimise kord;
15) sissepääsuloa või sissepääsu tagava vahendi kaotamise, kaotamiskahtluse või muu valduse kaotamisest teavitamise kord;
16) selle isiku määramine, kellele tuleb anda hoiule konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandja säilitamiseks kasutatava seifi luku varuvõti ja luku kood.

(2) Lisaks lõikes 1 nimetatutele võib riigisaladuse kaitse juhendis sätestada näiteks:
1) töötleva üksuse piires salastatud teabekandjate vastuvõtmise ja edastamise korra (turvaala piires, administratiivala kaudu);
2) salastatud teabekandjate edastamise täpsema korra;
3) salastatud teabekandjate reprodutseerimise korra;
4) kohapealse mehitatud valve kontrollkäikude korra;
5) turvaalale iseseisva sissepääsuõigusega isikute sissepääsuloa erisused võrreldes samas töötlevas üksuses töötavate isikutega;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
6) külalise turvaalale lubamise erisused võrreldes samas töötlevas üksuses töötavate isikutega;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

7) riigisaladuse töötlussüsteemi turvanõuete rakendamise juhendi kehtestamine.

(3) Riigisaladuse kaitse juhendi osa, mis peab olema salastatud, kehtestatakse juhendi lisana või eraldi dokumendina.

§ 23. Salastatud teavet valdava asutuse, põhiseadusliku institutsiooni ja juriidilise isiku riigisaladuse kaitset korraldava isiku või struktuuriüksuse tegevusele esitatavad nõuded

Salastatud teavet valdava asutuse, põhiseadusliku institutsiooni ja juriidilise isiku riigisaladuse kaitset korraldav isik või struktuuriüksus peab:
1) korraldama salastatud teabe kaitset ning «Riigisaladuse ja salastatud välisteabe seaduse» ja selle alusel antud aktide nõuetest kinnipidamist;
2) nõustama töötajaid salastatud teabe töötlemisel;
3) korraldama juurdepääsuõigust omavate isikute koolitust salastatud teabe kaitse küsimustes, sealhulgas elektroonilise teabeturbe alal;
4) korraldama turvaala valvurite tööd ja teostama järelevalvet nende tegevuse üle, kui seda ülesannet ei ole antud teisele ametiisikule;
5) kontrollima nõusolekute, kinnituste, juurdepääsuloa ja töötlemisloa ning nende kehtivuse pikendamise taotluste ning juurdepääsuloa ja töötlemisloa taotleja ankeedi vormilist nõuetele vastavust enne edastamist;
6) pidama arvestust töötajate riigisaladusele juurdepääsu lubade ja juurdepääsusertifikaatide üle;
7) pidama arvestust salastatud teabekandjate üle;
8) pidama seifide kasutajate nimekirja;
9) edastama iga 90 päeva järel vastavalt Kaitsepolitseiametile, Kaitseväele või Välisluureametile info juurdepääsuluba mitteomavate isikute ametisse nimetamisest ametikohale, millel on ette nähtud piiratud tasemel riigisaladusele juurdepääsu õigus, samuti sellisel ametikohal oleva isiku ametikohalt vabastamisest ning teenistusvälistele isikutele piiratud taseme riigisaladusele juurdepääsu lubamise otsustamisest;
[RT I, 19.08.2014, 17- jõust. 22.08.2014]
10) korraldama elektroonilise teabeturbe nõuete täitmist ja andma Välisluureametile sellekohast teavet viimase nõudmisel;
11) turvanõuete rakendamise juhendi kohaselt dokumenteerima teabe töötlussüsteemide ja nende osade kohta;
12) töötama koostöös süsteemi- ja võrguhalduritega välja süsteemi turvanõuete rakendamise juhendi ning tagama selle tutvustamise ja kättesaadavuse;
13) määrama kindlaks isikud, kes omavad töötlussüsteemile või selle osale juurdepääsu õigust, ning juurdepääsuõiguse sisu ja ulatuse, kui seda ei ole määranud töötleva üksuse juht;
14) väljastama salasõnu ja muid teabele juurdepääsu andvaid füüsilisi ja elektroonilisi vahendeid ning tagama selliste vahendite perioodilise vahetamise ja nende üle arvestuse pidamise;
15) jälgima ja dokumenteerima töötlussüsteemide hooldamist ja remontimist ning nende konfiguratsiooni muutmist;
16) pidama arvestust salastatud teavet sisaldavate töötlussüsteemi osade, sealhulgas irdmeedia ja muude salvestuskandjate ja nende kasutajate üle ning kontrollima perioodiliselt salvestuskandjate tegelikku olemasolu, sisu, hoiutingimusi ja märgistust;
[RT I 2008, 55, 312- jõust. 01.01.2009]
17) selgitama välja sündmuse või protsessi mittetoimumise või töötlussüsteemi volitustevastase kasutamise asjaolud;
18) teavitama viivitamatult Kaitsepolitseiametit ja vastavalt Kaitseväge, Välisluureametit või riigi julgeoleku volitatud esindajat, kui talle on teatavaks saanud «Riigisaladuse ja salastatud välisteabe seaduse» ning selle alusel antud õigusaktidest tulenevate nõuete rikkumine või teabe teatavaks saamine vastava taseme juurdepääsuõigust mitteomavale isikule;
[RT I, 19.08.2014, 17- jõust. 22.08.2014]
18^{1}) teavitama viivitamata käesoleva määruse § 103 lõikes 2 sätestatud erandi kasutamisest ja seda kasutanud isikust kirjalikult Kaitsepolitseiametit ning salastatud välisteabe edastamise korral riigi julgeoleku volitatud esindajat, välja arvatud riigisaladuse ja salastatud välisteabe seaduse § 52 lõikes 3 sätestatud juhul;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
18^{2}) korraldama nende teavituste säilitamise ja hävitamise, mis on esitatud sellistesse välisriikidesse reisimise kohta, mille kohta kehtib teatamiskohustus;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
19) võtma seletusi isikutelt, kes on rikkunud «Riigisaladuse ja salastatud välisteabe seaduse» või selle alusel antud õigusakti nõudeid.

5. peatükk
SALASTATUD TEABE JA SALASTATUD TEABEKANDJA TÖÖTLEMISE NÕUDED

1. jagu

Turvaala

1. jaotis
Turvaala üldnõuded

§ 24. Turvaala üldnõuded

(1) Turvaalal peab olema määratletud ja kaitstud välispiir, millel on võimalik kontrollida kõiki sisse- ja väljapääse, ning sisse- ja väljapääsukontrolli süsteem, mis võimaldab turvaalale iseseisvalt siseneda ainult nõutava tasemega juurdepääsuõigusega isikul.

(2) Ala turvaalana kasutamine peab olema eelnevalt kooskõlastatud vastavalt Kaitsepolitseiameti, Kaitseväe või Välisluureametiga.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

(3) Kaitsepolitseiamet, Kaitsevägi või Välisluureamet võivad teha käesolevas määruses sätestatud turvaalale esitatavates nõuetes konkreetse hoone või töötleva üksuse suhtes erandeid, kui nõuete rakendamine ei ole tehniliselt või seadusest tulenevatel põhjustel võimalik või kui turvaala nõuetekohasuse võib tagada muude meetmete abil.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

(4) Turvaala üldisi nõudeid kohaldatakse ajutisele ja liikuvale turvaalale niivõrd, kuivõrd käesolevas määruses ei ole sätestatud teisiti.

(5) Ala turvaalana kasutamise lõpetamisel tuleb sellest teavitada kooskõlastanud asutust 30 päeva jooksul kasutamise lõpetamisest arvates.

§ 25. Turvaala asukoht

(1) Turvaala peab asuma riigisaladust valdava töötleva üksuse otseses valduses olevates ruumides. Väljaspool töötleva üksuse otseses valduses olevat turvaala võib teavet töödelda ainult konkreetsele teabele juurdepääsuvajadust ja õigust omava töötleva üksuse turvaalal.

(2) Enne turvaala rajamise planeerimist tuleb konsulteerida kooskõlastamiseks pädeva asutuse esindajatega, et määrata turvaala parim asukoht hoones.

(3) Võimaluse korral ei rajata turvaala hoone esimesele ega viimasele korrusele.

(4) Võimaluse korral tuleb turvaala asukoht hoones valida selliselt, et akende olemasolul avaneksid need riigisaladust töötleva asutuse valduses olevale territooriumile.

(5) Riigisaladust ja salastatud teabekandjaid töötlevad isikud ja struktuuriüksused tuleb võimaluse korral paigutada asutuses lähestikku, näiteks ühte ja samasse ruumi või hoone ühte tiiba.

§ 26. Liikuv ja ajutine turvaala

(1) Erandkorras võib turvaala rajada ka liikuvatele platvormidele (edaspidi *liikuv turvaala*) või aladele, mis tavaliselt ei ole kasutuses turvaalana (edaspidi *ajutine turvaala*). Liikuvaks ja ajutiseks turvaalaks võib olla näiteks sõiduk, haagis, laev, punker, konteiner, soojak, telk, ülesande täitmiseks sobiv olemasolev ehitis. Võimaluse korral tuleb ajutise turvaalana kasutada püsiehitist.
[RT I 2008, 55, 312- jõust. 01.01.2009]

(2) Sellise turvaala kasutusele võtmine tuleb eelnevalt kooskõlastada vastavalt Kaitsepolitseiameti, Kaitseväe või Välisluureametiga, salastatud välisteabega turvaala korral ka riigi julgeoleku volitatud esindajaga. Liikuva või ajutise turvaala kooskõlastamist taotleval asutusel tuleb kooskõlastuse saamiseks esitada kooskõlastavale asutusele kirjalik taotlus vähemalt 30 päeva enne sellise turvaala kasutusele võtmist.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

(2^1) Julgeolekuasutus võib võtta liikuva või ajutise turvaala kasutusele oma juhi või tema volitatud isiku otsusel ilma lõikes 2 sätestatud teise julgeolekuasutuse kooskõlastuseta. Liikuva või ajutise turvaala, millel töödeldakse salastatud välisteavet, kasutusele võtmine tuleb ka sel juhul kooskõlastada riigi julgeoleku volitatud esindajaga. Liikuva või ajutise turvaala kasutuselevõtmisel teavitab julgeolekuasutus teist julgeolekuasutust kirjalikult esimesel võimalusel.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(3) Kiireloomulistel asjaoludel võib lõikes 2 nimetatud tähtaega lühendada kooskõlastava asutuse nõusolekul.

(4) Liikuvale ja ajutisele turvaalale kohaldatakse võimalusel kõiki turvaala nõudeid, võimaluse puudumisel tagatakse salastatud teabe turvalisus muude meetmetega.

(5) Eriolukorra, erakorralise seisukorra, kõrgendatud kaitsevalmiduse, sõjaseisukorra, mobilisatsiooni ja demobilisatsiooni ajal võib liikuva või ajutise turvaala luua iga riigisaladust või salastatud välisteavet valdava asutuse juhi suulise korralduse alusel. Suuliselt antud korraldus tuleb esimesel võimalusel ka kirjalikult jäädvustada. Asutused, kelle tegevus eeldab nimetatud olukordades liikuva või ajutise turvaala loomist, peavad kajastama sellekohase info asutuse ja teiste tasandite, näiteks maakonna ja ministeeriumi kriisiplaanides ning teavitama sellest kooskõlastavat asutust.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(6) Liikuval ja ajutisel turvaalal töödeldakse vaid konkreetse ülesande täitmiseks vajalikke salastatud teabekandjaid. Kui töötlemisvajadus on lõppenud, viiakse salastatud teabekandjad viivitamata alalisele turvaalale.

(7) Liikuva või ajutise turvaala koha valikul tuleb eelkõige arvestada ülesande tõhusat ja turvalist täitmist.

(8) Asutuse juht peab määrama isiku, kes vastutab liikuval või ajutisel turvaalal salastatud teabekandjate kaitseks rakendatavate julgeolekumeetmete eest (edaspidi *vastutav isik*).

(9) Kui turvaala kasutamisel ilmneb lahknevusi eelnevalt kooskõlastamisele esitatud andmetest, siis tuleb vastutaval isikul sellest kirjalikult teavitada kooskõlastavat asutust hiljemalt 30 päeva pärast muudatuse toimumist.

§ 27. Turvaala sein, lagi ja põrand

(1) Turvaala sein, lagi ja põrand peavad olema valmistatud betoonist, terasest või kivist nii, et detaile, millest sein, lagi või põrand koosneb, ei oleks võimalik väljastpoolt lihtsalt eemaldada.

(2) Kahe turvaala vaheline sein või turvaala sisesein võivad olla kergkonstruktsiooniga. Turvaala välissein, lagi või põrand võib olla kergkonstruktsiooniga, kui hoones on pidev mehitatud valve või kui neid on tugevdatud füüsiliste tõkete lisamisega või tehniliste valveseadmetega.

(3) Turvaala helipidavus peab olema selline, et seal toimuv ei kostaks ümbritsevatesse ruumidesse.

§ 28. Turvaala uks

(1) Turvaala välispiiril asuv uks (edaspidi *turvaala uks*) peab olema kooskõlastava asutuse hinnangul piisavalt turvaline, et valvepersonal jõuaks sissetungikatsele reageerida enne, kui sissetungija on ületanud füüsilised tõkked.

(2) Turvaala ukse hingedepoolsel küljel peavad olema turvatapid, mis ukse sulgemisel sulguvad lengi sisse. Turvaala uksel peab olema automaatne sulgur, mis tagab ukse iseenesliku sulgumise määratud aja jooksul, ja andur, mis annab märguande, kui uks on olnud avatud üle määratud aja.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(3) Kui nõuetekohast turvaala ust ei ole võimalik paigaldada, tuleb turvaala ust valvata täiendavate valve- ja häiresüsteemiseadmetega.

(4) Turvaala uks peab olema varustatud vähemalt kahe lukuga, millest vähemalt üks peab olema automaatselt lukustuv ja vähemalt üks mehaaniline turvalukk. Turvaluku keel peab olema kaitstud.

(5) Turvaala mehaanilised ukselukud ei tohi olla avatavad sama võtmega, millega saab avada hoones asuvaid teisi mehaanilisi ukselukke. Kui seda nõuet ei ole võimalik järgida, tuleb võtmeid hoida samadel tingimustel seifivõtmetega.

§ 29. Turvaala aken

(1) Kergesti ligipääsetavas kohas, näiteks katusel, rõdul ja hoonelaiendusel asuv turvaala aken tuleb varustada sissemurdmist takistavate turvaelementidega. Vajaduse korral tuleb kasutada akna turvalisuse suurendamiseks muid füüsilisi tõkkeid või valve- ja häiresüsteemiseadmeid.

(2) Turvaala aken tuleb katta kardina või toonkilega, et väljastpoolt ei oleks võimalik jälgida turvaalal toimuvat.

§ 30. Turvaala muu avaus

Turvaalal asuv muu avaus peab olema kaitstud füüsiliste tõkete või valve- ja häiresüsteemiseadmetega, et välistada turvaalale tehniliste seadmete ebaseaduslik paigaldamine või turvaalal hoitaval salastatud teabekandjal sisalduva teabe muul viisil ohustamine.

§ 31. Avatud hoiuala

Avatud hoiuala välissein, lagi ega põrand ei tohi olla kergkonstruktsiooniga.

§ 32. Liikuva ja ajutise turvaala konstruktsiooniline kaitse

(1) Liikuval ja ajutisel turvaalal peab olema füüsilise tõkkega selgelt määratud ja kaitstud välispiire, milles on võimalik kontrollida kõiki sisse- ja väljapääse. Kooskõlastava asutuse nõudel peab muutma turvaala asukohta, tugevdama turvaala konstruktsiooni ja kasutama lisapiirdeid.

(2) Liikuva ja ajutise turvaala konstruktsioon peab tagama, et väljastpoolt oleks välistatud juurdepääs salastatud teabele või selle ohustamine.

§ 33. Evakuatsiooniplaan

(1) Turvaala kohta peab olema koostatud ohuolukorras tegutsemiseks salastatud teabekandjate evakuatsiooniplaan.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(2) Evakuatsiooniplaanis peavad olema kajastatud erinevad võimalikud ohuolukorrad, millal tuleb salastatud teabekandjad evakueerida või hävitada.

(3) Lõike 2 alusel määratletud iga ohuolukorra kohta tuleb ette näha, kuidas toimub evakuatsioon või hävitamine, kellel on õigus anda selleks korraldus, kes seda läbi viib, milliseid vahendeid selleks kasutatakse, kuhu evakueeritakse salastatud teabekandjad.

2. jaotis
Turvaala valve nõuded

§ 34. Turvaala valve üldnõuded

(1) Turvaalal peab olema sissetungimisvastane häiresüsteem (edaspidi *häiresüsteem*) ja kohapealne mehitatud valve.

(2) Kohapealse mehitatud valve nõue ei kehti juhul, kui turvaala tehniline valve ja füüsilise kaitse meetmed võimaldavad mehitatud valvel reageerida sissetungikatsele enne, kui sissetungija on ületanud füüsilised tõkked.

(3) Turvaala või selle osa peab olema valve all, kui sellel ei viibita.

§ 35. Tehnilise valve süsteemi nõuded

(1) Tehnilise valve süsteem peab:
1) andma häire, kui toimub sissetung või selle katse;
2) olema selline, et mehitatud valve jõuaks reageerida enne, kui sissetungija on ületanud füüsilised tõkked;
3) võimaldama turvaala valvet eraldi sisse ja välja lülitada, sisse- ja väljalülitamist ning häire aega hiljem elektrooniliselt tuvastada. Neid toiminguid kajastavaid andmeid tuleb säilitada vähemalt üks aasta;
4) automaatselt tuvastama süsteemi rikked.

(2) Tehnilise valve süsteemi rikke korral peab süsteem andma kohe häire mehitatud valvele.

(3) Riigisaladuse kaitseks kasutatava tehnilise valve süsteemi reservtoide peab tagama süsteemi toimimise põhielektrisüsteemi tõrke korral turvaala mehitatud valve alla võtmiseni.

§ 36. Liikuva ja ajutise turvaala mehitatud valve

(1) Liikuvat või ajutist turvaala peavad kaitsma liikuvad või püsipositsioonidel relvastatud valvurid, kes jälgivad kogu kaitstavat ala. Sellest nõudest võib teha erandeid ainult kooskõlastava asutuse loal lähtuvalt turvaala asukohale antud ohuhinnangust. Turvaala valvamiseks võib kasutada nii valvemeeskonna valvureid kui ka turvaalal ööpäevaringselt töötavaid instrueeritud isikuid.

(2) Kui liikuva või ajutise turvaala pidevat mehitatust ei suudeta tagada, siis tuleb liikuvale või ajutisele turvaalale paigaldada häiresüsteem, mis edastab häiresignaali instrueeritud isikutele, s.t valvemeeskonnale või turvaala töötajatele, kes peavad jõudma turvaalale kooskõlastava asutusega kooskõlastatud reageerimisaja jooksul. Reageerimisaeg ei tohi olla pikem ajast, mis kulub sissetungijal füüsiliste tõkete ületamiseks.

§ 37. Kohapealse mehitatud valve ringkäigud

(1) Kohapealse mehitatud valve ringkäigud peavad väljaspool tööaega, puhkepäevadel ja riigipühadel toimuma eri intervalliga. Ringkäikude intervall ei tohi ületada kahte tundi, välja arvatud valvekaamerate kasutamise korral.

(2) Kohapealne mehitatud valve peab kindlaks tegema kõik turvaalal töötavad isikud ja nende tööruumid. Igal järgmisel ringkäigul tuleb üle kontrollida need ruumid, kus viimase ringkäigu ajal isikud töötasid.

(3) Järgmistel ringkäikudel peab kohapealne mehitatud valve jälgima, et juhuslikult valitud ruumide kontrollimise käigus oleksid kolme ringkäiguga üle kontrollitud kõik ruumid. Samuti peab ringkäigul kontrollima, et turvaalal ei oleks ühtegi märki sissetungijatest ning kõik ringkäigu marsruudile jäävad uksed, aknad ja muud sissepääsud turvaalale on suletud ja puutumata.

(4) Juurdepääsuõigusest ja teadmisvajaduse nõudest lähtuvalt võib töötleva üksuse juht piirata mehitatud valve sissepääsu turvaalale või selle osale.

§ 38. Kohapealse mehitatud valve õigus juurdepääsuks riigisaladusele

Turvaalal ringkäiku tegeval kohapealsel mehitatud valvel peab olema vähemalt selle taseme riigisaladusele juurdepääsu luba, mis tasemel salastatud teavet kontrollitaval turvaalal töödeldakse.

3. jaotis
Isikute viibimine ja töötamine turvaalal

§ 39. Isikute viibimine turvaalal

Isikute turvaalal viibimise korraldus peab arvestama isiku riigisaladusele juurdepääsu õigust, teadmisvajadust ning tegema kindlaks isiku turvaalale sisenemise ja sealt väljumise.

§ 40. Iseseisva sissepääsuõigusega isiku pääs turvaalale

(1) Turvaalale iseseisva sissepääsuõigusega isikule antakse sissepääsuluba, millele kantakse loa number. Sissepääsuluba ei pea andma, kui turvaala koosneb ühest või kahest ruumist.

(2) Töötlev üksus peab pidama arvestust turvaalale pääsevate isikute sissepääsuõiguse, sissepääsu tagavate vahendite ja sissepääsulubade üle.

(3) Turvaalal töötav isik kannab sissepääsuluba nähtaval kohal, et oleks võimalik tuvastada tema isik. Sissepääsuloa nähtaval kohal kandmise nõue ei kehti julgeolekuasutuste puhul. Väljaspool turvaala ja administratiivala ei tohi sissepääsuluba nähtaval kohal kanda.

(4) Turvaala sisse- ja väljapääsukorraldus peab tagama iseseisva sissepääsuõigusega isikute tuvastamise sisenemisel ja väljumisel.

(5) Sissepääsuloa või sissepääsu tagava eseme kaotamise, kaotamiskahtluse või muu valduse kaotuse korral tuleb sellest viivitamata teavitada töötlevas üksuses määratud isikut, kes võtab meetmed sissepääsuloa või sissepääsu tagava eseme kasutamise takistamiseks.

§ 41. Külalise viibimine turvaalal

(1) Turvaalale võib lubada külalise töötleva üksuse riigisaladuse kaitse juhendis sätestatud korras.

(2) Külalisele antakse numbriga külastusluba, millele on märgitud sõna «KÜLALINE» ja mis võimaldab tuvastada loa saanud isiku. Külaline peab kandma külastusluba nähtaval kohal.

(3) Külastusluba ei pea väljastama, kui turvaala koosneb ühest või kahest ruumist.

(4) Külastusloa andmine ja selle tagastamine, külalise saabumise ja lahkumise aeg, külalise ees- ja perekonnanimi tuleb registreerida. Külaline tuleb identifitseerida kehtiva isikut tõendava dokumendi alusel.

(5) Külaline võib turvaalal liikuda üksnes koos vastuvõtjaga või temale määratud saatjaga. Külalist on keelatud jätta turvaalale üksinda, välja arvatud juhul, kui külalisel on õigus juurde pääseda selle taseme riigisaladusele, mida turvaalal töödeldakse, ning arvestades teadmisvajaduse põhimõtet.

§ 42. Liikuval ja ajutisel turvalal töötamise nõuded

(1) Ajutise turvaala eest vastutav isik peab turvaala kolimise korral hüljatud turvaala üle vaatama ja veenduma, et alale ei ole jäänud salastatud teabekandjaid.

(2) Kui töö ajutisel turvaalal on lõppenud, tuleb salastatud teabekandjad toimetada asutuse alalisele turvaalale andmete võrdlemiseks ja eesmärgi täitnud materjali hävitamiseks.

(3) Ajutise turvaala olemasolevaid füüsilise julgeoleku meetmeid tuleb vajaduse korral tugevdada ka pärast seda, kui turvaala kasutamine on kooskõlastatud.

4. jaotis
Salastatud teavet käsitleva koosoleku pidamise nõuded

§ 43. Koosoleku pidamise üldnõuded

Salastatud teavet käsitleva nõupidamise, koosoleku, konverentsi või muu kohtumise (edaspidi *koosolek*) korraldamiseks peavad olema täidetud järgmised nõuded:
1) salastatud teavet käsitleva koosoleku korraldaja peab tagama, et koosolekule on juurdepääs ainult isikutel, kellel on käsitletava taseme salastatud teabele juurdepääsu õigus ning teadmisvajadus;
2) koosolekuruumis toimuvat ei või olla võimalik väljastpoolt näha ega kuulda.

§ 44. Koosoleku pidamine turvaalal ja administratiivalal

(1) Koosoleku pidamiseks kasutatavad ruumid peavad asuma turvaalal.

(2) Piiratud taseme riigisaladust käsitleva koosoleku läbiviimiseks kasutatavad ruumid võivad asuda ka administratiivalal ja neile ei pea kohaldama käesolevas jaos järgnevalt sätestatud nõudeid.

§ 45. Koosolekuruumide perioodiline kontrollimine

Koosolekuruume tuleb perioodiliselt kontrollida, et vältida lubamatut audio- või videosalvestamist. Koosolekuruumis ei tohi koosoleku toimumise ajal olla ühtegi tehnilist vahendit ega eset, mis on eelnevalt kontrollimata või mida saab kasutada pealtkuulamiseks või lubamatuks salvestamiseks.

§ 46. Koosolekul tehtud märkmete registreerimine

Iga koosolekul osaleja poolt koosolekul tehtud märkmed, kokkuvõtted ja muu sellise materjali vaatab läbi ja tagastab või edastab koosoleku korraldaja osalejatele alles siis, kui riigisaladust sisaldavad märkmed on märgistatud ja registreeritud.

2. jagu
Salastatud teabekandjate arvestus

§ 47. Salastatud teabekandjate registreerimise üldnõuded

Salastatud teabekandja registreerimisel juhindutakse avaliku teabe seadusest ning avaliku teabe seaduse ja arhiiviseaduse alusel antud õigusaktidest ja juhistest käesolevas määruses sätestatud erisustega.
[RT I, 31.05.2017, 7- jõust. 03.06.2017]

§ 48. Dokumendi originaal

Mitmes eksemplaris loodud salastatud dokumendi originaaliks loetakse dokumendi esimest eksemplari. Muid eksemplare käsitatakse ja töödeldakse koopiatena.

§ 49. Salastatud teabekandjate register

(1) Salastatud teabekandjate registreerimiseks peavad riigisaladust valdavad asutused, põhiseaduslikud institutsioonid ja isikud sisse seadma salastatud teabekandjate registri (edaspidi *register*).

(2) Olenevalt salastatud teabekandjate hulgast võib sisse seada eraldi registrid täiesti salajase, salajase, konfidentsiaalse ja piiratud taseme salastatud teabekandjate registreerimiseks.

(3) Piiratud tasemel salastatud teabekandjaid võib töötleva üksuse juhi otsusega registreerida ka üldises dokumendiregistris, kui on tagatud, et salastatud teave ei saa seetõttu teatavaks kõrvalistele isikutele.

(4) Salastatud teabekandjate allregistri võib töötleva üksuse juhi otsusega sisse seada asutuse igas struktuuriüksuses.

§ 50. Nõuded registrile

(1) Salastatud teabekandjate registrit võib pidada elektrooniliselt või paberil.

(2) Registrikanne ise ei tohi võimaluse korral sisaldada salastatud teavet.

(3) Töötlev üksus peab tagama registriandmete alalise säilimise.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

§ 51. Registrisse kantav teave

(1) Salastatud teabekandjate registrisse märgitakse:
1) teabekandja identifitseerimiseks vajalikud andmed: registreerimisnumber, registreerimise kuupäev, koostamise kuupäev, selle asutuse nimetus, kust teabekandja on saabunud, ja edastaja registreerimisnumber, dokumendi puhul ka pealkiri ning dokumendi koostaja ja allkirjastaja. Koopiale ei pea andma uut registreerimisnumbrit, kui märgitakse koopia järjekorranumber;
2) teabekandja liik;
3) teabekandja salastamise alus, salastatuse tase ja tähtaeg, nende muudatus ja muudatuse tegemise alus;
4) eksemplaride arv ja numbrid; eksemplaride arvu ei pea registrisse kandma piiratud ja konfidentsiaalsel tasemel salastatud teabekandja puhul;
5) teabekandja osade ja dokumendi lehtede arv. Kui dokument on vormistatud lehe mõlemale küljele, registreeritakse salastatud teabekandjate registris selle dokumendi lehtede arv, märkides juurde, et dokument on vormistatud lehe mõlemale küljele;
6) koopiate arv; koopiate arvu ei pea registrisse kandma konfidentsiaalsel ja madalamal tasemel salastatud teabekandja puhul;
7) selle töötleva üksuse nimetus, kellele salastatud teabekandja või selle koopia on edastatud, ning edastamise aeg; vastuvõtja allkiri või üleandmis-vastuvõtmisakti number;
8) märge selle kohta, kui teisele töötlevale üksusele on antud luba edastada salastatud teabekandjal sisalduvat salastatud teavet kolmandale töötlevale üksusele;
9) märge hävitamise kohta;
10) selle isiku nimi, kellele salajasel või kõrgemal tasemel salastatud teabekandja edastati või kellele seda tutvustati, ning edastamise või tutvustamise aeg.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(2) Teisaldatavate elektrooniliste salvestuskandjate kohta märgitakse salastatud teabekandjate registrisse:
1) salvestuskandja liik – näiteks kõvaketas, mälupulk;
[RT I, 14.01.2011, 6- jõust. 17.01.2011]
2) registreerimisnumber;
3) registreerimise kuupäev;
4) salvestuskandjal sisalduva teabe kõrgeim salastatuse tase;
5) töötlev üksus, kellele salvestuskandja edastati, edastamise aeg.

§ 52. Salastatud teabekandjate registreerimine

(1) Salastatud teabekandja registreeritakse selle koostamise või saabumise päeval.

(2) Salastatud teabekandja registreeritakse üldjuhul üks kord. Põhiregistris registreeritud salastatud teabekandjat ei pea registreerima sama töötleva üksuse allregistris.

(3) Kui salastatud dokumentide kogum sisaldab ka salastamata teabekandjaid, võib kogumisse kuuluvad salastamata teabekandjad registreerida salastatud teabekandjate registris. Kui kogum koosneb eraldi kasutatavatest salastatud dokumentidest, võib iga kogumi osaks oleva dokumendi registreerida eraldi.

(4) Kui teabekandja sisaldab nii riigisaladust kui ka salastatud välisteavet, registreeritakse teabekandja vastava taseme riigisaladuse registris.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

§ 53. Registripidaja

Registrisse kandeid tegeval isikul (edaspidi *registripidaja*) peab olema registreeritavate teabekandjate kõrgeimale salastatuse tasemele juurdepääsu õigus. Registripidaja või registripidajad ja vajaduse korral nende asendajad määrab töötleva üksuse juht.

§ 54. Salastatud teabekandjaga tutvumise kinnitus

(1) Salajasel ja kõrgemal tasemel salastatud teabekandjas sisalduva teabega tutvumise kohta tehakse vastav märge. Paberteabekandjaga tutvumise kohta annab tutvuja allkirja teabekandja juures olevale tutvumislehele või teabekandjale endale. Elektroonilise teabekandjaga võimaldatakse tutvuda, kui elektrooniliselt tagatakse tutvuja isikusamasuse ja tutvumisaja tuvastatavus.

(2) Andmeid teabekandjaga tutvumise kohta säilitatakse sama kaua kui registriandmeid. Tutvumislehti ja muid andmeid teabekandjaga tutvumise kohta säilitatakse sama kaua kui registriandmeid.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

3. jagu

Salastatud teabekandja märgistamine

1. jaotis
Märgistamise üldnõuded

§ 55. Riigisaladust sisaldava salastatud teabekandja märgistamine

(1) Kui märgistamine ei sea ohtu riigisaladuse salastatust, tuleb teha salastatud teabekandjale selgelt nähtav salastusmärge «täiesti salajane», «salajane», «konfidentsiaalne» või «piiratud»:
1) sõrendatud paksus kirjas, vähemalt 16-punktiste suurtähtedega trükituna või
2) punaselt sama suurusega ja samal kujul templijäljendiga, kleepsuga või muul sellisel viisil.

(2) Kui teabekandja suuruse tõttu ei ole võimalik seda märgistada, võib märgistuse kanda teabekandja külge kinnitatud sildile. Väikeste teabekandjate puhul võib põhjendatud juhtudel märgistus olla väiksem lõike 1 punktis 1 sätestatust, tingimusel et märgistus on hõlpsasti nähtav ja loetav.

(3) Riigisaladust sisaldavale salastatud teabekandjale märgitakse ka teabe salastamise alus järgmisel kujul: «Riigisaladus … alusel». Lünka tuleb märkida viide käesolevale määrusele, vastavale paragrahvile, lõikele ja punktile. Kui salastatud teabekandja on salastatud mitmel alusel, tuleb teabekandjale märkida kõik alused.

(4) Salastatud teabekandjale tuleb veel märkida teabekandja registreerimise kuupäev, number ja salastamistähtaeg.

(5) Teabekandja üldine salastatus peab vastama selle osade kõrgeimale salastatuse tasemele.

(6) Riigisaladust sisaldava teabekandja edastamisel välisriigile või rahvusvahelisele organisatsioonile kantakse teabekandjale välislepingu nõuetele vastavad salastusmärked ning esilehele inglise keeles märge ka selle kohta, et tegemist on Eesti Vabariigi teabega.

§ 56. Salastatud välisteavet sisaldava teabekandja märgistamine

(1) Salastatud välisteavet sisaldava teabekandja esimesele lehele kantakse salastatud välisteabe avaldaja salastatuse taseme märgistus, kui see on välislepinguga ette nähtud, ja sellele vastava taseme riigisaladuse märgistus.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(2) Teabekandja esilehe ülemisse paremasse nurka tehakse täiendav märge „Salastatud välisteave“ suurtähtedega ja märgitakse salastatud välisteabe avaldaja nimi, salastatuse tase ja tähtaeg, kui välisteabe avaldaja on tähtaja märkinud.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(3) Juhul kui teabekandja sisaldab mitme avaldaja salastatud välisteavet, tehakse lõikes 2 sätestatud märge iga teabeavaldaja kohta eraldi.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(4) Eri avaldajate teavet võib märgistada tekstilõikude ja illustratsioonide kaupa, tehes avaldaja salastatuse taseme märke lõigu esimese rea algusesse ja viimase rea lõppu või illustratsiooni ette ja järele. Avaldaja ja salastatuse taseme märge kirjutatakse suurtähtedega paksus kirjas nurk- või looksulgudes.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(5) Riigi julgeoleku volitatud esindaja kirjalikul nõusolekul võib elektroonilise teabe jätta lõigetes 1–3 sätestatud nõuete kohaselt märgistamata, kui teave on märgistatud § 70 lõikes 1 sätestatud korras.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

§ 57. Salastatud teabekandja koopia ja väljavõtte märgistamine

(1) Koopiale märgitakse «KOOPIA». Kui dokumendi originaalil olevad märked ei kandu reprodutseerimisel automaatselt üle koopiale, kantakse koopiale samad märked, mis on originaalil.

(2) Väljavõttele märgitakse «VÄLJAVÕTE», millisest originaaldokumendist on väljavõte tehtud ja originaali salastamismärked.

§ 58. Lisamärgistus turvameetmete ja juurdepääsuõigust omavate isikute kohta

(1) Kui teabekandja märgistatakse lisatähisega täiendavate turvameetmete või teabekandjale juurdepääsu õigust omavate isikute ringi kohta, tehakse vastav märge salastamisaluse märke juurde.

(2) Salastatud krüptomaterjalidele tehakse lisamärge «KRÜPTO».

§ 59. Pakendatud teabekandja täiendavad salastusmärked

(1) Kui salastatud teabekandjat või andmekogumit säilitatakse kokkupakituna, -rullituna, konteinerisse või karpi panduna või muul viisil nii, et pakend varjab salastusmärget, tuleb teabekandjale või pakendile teha täiendavad salastusmärked selliselt, et asjaolu, et tegemist on riigisaladust sisaldava teabekandjaga, on tuvastatav nii pakitud kui lahtipakitud teabekandja korral kui ka teabekandjat töödeldes.

(2) Teabekandja pakendamisel selle edastamiseks kohaldatakse käesoleva peatüki 7. jao sätteid.

§ 60. Märgistuse kustutamine ja muutmine

(1) Salastatuse kustumisel salastamistähtaja möödumisel kriipsutatakse salastusmärge läbi.

(2) Salastatuse ennetähtaegsel kustutamisel kriipsutatakse salastusmärge läbi ning märgitakse salastamise aluse märke juurde «Salastatus kustutatud … alusel», viidates kustutamise otsuse teinud organile, otsuse rekvisiitidele ja otsuse jõustumise ajale.

(3) Salastamistähtaja pikendamisel märgitakse salastamise aluse märke juurde «Salastamistähtaeg pikendatud … alusel», viidates pikendamise otsuse teinud organile ja otsuse rekvisiitidele, ning märgitakse uus salastamistähtaeg.

(4) Salastamisandmete parandamisel kriipsutatakse vale märgistus läbi ja selle alla märgitakse «Salastatus parandatud …» vastavalt salastamisandmete parandamise otsusele. Juurde märgitakse otsuse teinud organi nimetus ning otsuse rekvisiidid või otsuse teinud ametniku ametinimetus, nimi ja allkiri.

(4[1]) Kui salastusmärge muudetakse „Riigisaladuse ja salastatud välisteabe seaduse“ § 56 lõike 4 alusel, lähtutakse salastusmärke tegemisel käesoleva paragrahvi lõigetest 2–4, kuid otsuse asemel viidatakse „Riigisaladuse ja salastatud välisteabe seaduse“ § 56 lõikele 4.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(5) Uus märgistus tehakse üldises korras lõigetes 2–4 nimetatu juurde.

2. jaotis
Dokumendi märgistamine

§ 61. Dokumentide vormistamise üldnõuete kohaldamine

Salastatud dokumendi koostamisel ja vormistamisel juhindutakse dokumentide vormistamise üldnõuetest, arvestades käesolevast määrusest tulenevaid erisusi.

§ 62. Lehtede nummerdamine

Salastatud dokumendi lehed peavad olema nummerdatud alates esilehest, samuti tuleb igale dokumendi lehele märkida lehtede koguarv. Kui dokument on vormistatud lehe mõlemale küljele, tuleb nummerdada ja märkida vastavalt leheküljed.

§ 63. Dokumendi märgistamine

(1) Salastatud dokumendi esilehele tehakse üles paremale märge teabe salastamise taseme ja aluse, teabekandja registreerimise kuupäeva, numbri ning salastamistähtaja kohta. Kõikidele dokumendi lehtedele märgitakse salastusmärge lehe keskele ülemisse ja alumisse serva vastavalt lehel sisalduva teabe kõrgeimale salastatuse tasemele.

(2) Salastatud dokumendil tervikuna on tema eri osade kõrgeim riigisaladuse tase, mille kohta tehakse salastusmärge dokumendi esilehele, samuti tiitellehele, esi- ja tagakaanele, kui need on olemas.

§ 64. Dokumendi lisa märgistamine

Kui dokumendi lisa on kasutatav algdokumendita, tuleb see märgistada ja vormistada nagu eraldi dokument.

§ 65. Tekstilõikude ja illustratsioonide kaupa märgistamine

Kui teabekandja märgistatakse täiendavalt tekstilõikude ja illustratsioonide kaupa, tuleb salastatuse taseme märge teha salastatud lõigu esimese rea algusesse ja viimase rea lõppu või illustratsiooni ette ja järele. Salastatuse taseme märge kirjutatakse suurtähtedega paksus kirjas nurk- või looksulgudes. Salastatuse taseme märget võib lühendada, märkides salastatuse taseme esitähe.

§ 66. Märgistamine dokumendil oleva teabe salastatuse kustumisel ja salastamisandmete parandamisel

(1) Märge dokumendi salastatuse kustumise, ennetähtaegse kustutamise või salastamistähtaja pikendamise, samuti salastamisaluse ja -tähtaja muutmise kohta tehakse dokumendi esilehe ülemisse parempoolsesse nurka teabekandja salastamise aluse kohta tehtud märke juurde.

(2) Teistel lehtedel kriipsutatakse salastatuse kustumisel ja kustutamisel salastusmärge lehe all- ja ülaservas läbi.

§ 67. Dokumentide kogumi märgistamine

(1) Salastatud dokumentidest moodustatud kogum märgistatakse kogumis sisalduva kõrgeima taseme riigisaladuse märkega.

(2) Toimikuks liidetud või muul viisil kaante vahele kogutud kogumi puhul tehakse salastusmärge toimiku esi- ja tagakaane ülemisse ja alumisse serva.

(3) Muudel juhtudel tehakse salastusmärge kogumi esimeseks dokumendiks oleva dokumendi esimese lehe ülemisse ja alumisse serva.

(4) Kui kogumi esileht ei sisalda riigisaladust, tehakse dokumendi paremasse ülemisse nurka lisaks ka märge: «Märgistatud riigisaladusena kui kogumi esileht».

3. jaotis
Muu teabekandja märgistamine

§ 68. Salastatud foto, transparendi ja slaidi märgistamine

Salastatud foto, transparendi ja slaidi märgistamiseks tehakse salastusmärge igale fotole, transparendile või slaidile.

§ 69. Heli-, filmi- ja videosalvestise märgistamine

Heli-, filmi- ja videosalvestisel peab olema märgistus nii selle pakendil kui teabekandjal ning selguma ka teabekandja sisust selle kasutamisel.

4. jaotis
Elektroonilise teabe märgistamine

§ 70. Faili märgistamine

(1) Salastatud teavet sisaldava faili salastatuse tase märgitakse suurtähtedega faili nime algusesse, kui see on võimalik, ja faili metaandmetesse.

(2) Kui fail sisaldab dokumenti, siis märgistatakse lisaks failile ka failis sisalduv dokument dokumendi märgistamise nõuete kohaselt. Failis sisalduva dokumendi märgistamisel tuleb parimal võimalikul moel tagada, et salastusmärge oleks kestvalt nähtav riigisaladust sisaldava andmekogumi kuvamisel, projitseerimisel või muul viisil tajutavaks muutmisel.

§ 71. Elektrooniliste sõnumite märgistamine

(1) Elektrooniliste sõnumite salastatuse märge kantakse suurtähtedega sõnumi pealkirja ning sõnumi põhiosa algusesse ja lõppu dokumendi märgistamise nõuete kohaselt.

(2) Sõnumi pealkirja ei pea salastatuse märget kandma juhul, kui sõnumile lisatud salastatud teabekandja on krüpteeritud ja sõnumi krüpteerimata osa ega pealkiri ei sisalda riigisaladust.

4. jagu
Salastatud teabekandja säilitamine

1. jaotis

Säilitamistingimustele ja -vahenditele esitatavad nõuded

§ 72. Seif

(1) Konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandjaid tuleb säilitada koodlukuga seifis, mille murdmiskindlus vastab vähemalt standardi EVS-EN 1143-1 1. klassi nõuetele.

(2) Piiratud tasemel salastatud teabekandjat võib säilitada ka lukustatud kapis või sahtlis, mis on kaitstud kõrvaliste isikute juurdepääsu eest.

(3) Seif, milles säilitatakse konfidentsiaalsel või kõrgemal tasemel salastatud teabekandjat, peab paiknema turvaalal.

(4) Kui seifi kasutab mitu isikut, tuleb seif jagada füüsiliselt osadeks lähtuvalt teadmisvajaduse põhimõttest. Seifil peavad niisugusel juhul olema eraldi lukustatavad osad.

(5) Kooskõlastava asutuse loal võib salastatud teabekandjaid säilitada avatud hoiualal. Kooskõlastav asutus määrab sellel töödeldava teabe lubatud kõrgeima salastatuse taseme.

§ 73. Salastatud teabekandjate säilitamine nende kasutamise ajal

(1) Salastatud teabekandjad peavad pärast nende väljavõtmist seifist või muust säilituskohast olema pideva järelevalve all. Kui salastatud dokumente parajasti ei kasutata, tuleb neid hoida tühi lehekülg ülespoole või kinnikaetult.

(2) Ruumist lahkumisel peab salastatud teabekandja lukustama vastavalt salastatuse tasemele seifi, kappi või sahtlisse.

§ 74. Erandid üldistest säilitustingimustest

(1) Kui salastatud teabekandjate säilitamise nõudeid ei ole töötlevas üksuses võimalik täita, tuleb salastatud teabekandjad anda ajutisele hoiule riigiasutusele, kus salastatud teabekandjate säilitamise nõuded on täidetud.

(2) Kooskõlastav asutus võib lubada liikuval ja ajutisel turvaalal kasutada § 72 lõikes 1 sätestatust madalama murdvarguskindluse klassiga seife.

(3) Kooskõlastav asutus võib lubada erandjuhul kasutada salastatud teabekandjate säilitamiseks ka muid võimalusi, näiteks säilitamine pakendatuna vastuvõtva baasi või staabi turvaalal, lukustatavas metallkastis, nahktaskus või mujal.

(4) Salajasel või konfidentsiaalsel tasemel salastatud teabekandjat võib asutuse juhi loal erandjuhtudel lühiajaliselt, näiteks sobiva suurusega seifi hankimiseni, säilitada metallist dokumendikapis või sahtlis, kui hoidmispaik asub turvaalal ja on varustatud vähemalt ühe sulgemisrauaga või kolmeosalise võtmekombinatsiooniga lukuga.

2. jaotis
Säilituspaiga võtmete ja lukukoodide kaitse

§ 75. Seifi lukukood

(1) Seifi lukukoodi tohib teada ainult selle seifi kasutaja.

(2) Lukukood ei tohi koosneda numbrite või tähtede reast, mida on kerge ära arvata, näiteks tähtpäevade kuupäevad, telefoninumbrid, aritmeetilised jadad.

(3) Lukukoode peab muutma:
1) kasutaja vahetumisel;
2) pärast avamist kasutaja juuresolekuta;
3) kui on põhjust arvata, et kood on saanud teatavaks kõrvalisele isikule;
4) 12 kuu möödumisel viimasest muutmisest.

§ 76. Seifi võti ja lukk

(1) Tööajal asub seifi võti selle seifi kasutaja käes.

(2) Töökohalt lahkudes tuleb seifi võti sulgeda võtmete kappi.

(3) Seifi lukud tuleb vahetada, kui on põhjust arvata, et seifi võti on sattunud kõrvalise isiku kätte.

§ 77. Võtmete kapp

(1) Võtmete kapp peab olema metallist, lukustatav ja asuma pideva valve all.

(2) Kui võtmete kappi kasutab mitu isikut, peab olema tagatud, et kasutaja saab võtta ainult talle vajaliku võtme.

§ 78. Seifi võtme varueksemplari ja lukukoodi hoidmine

(1) Seifi võtme varueksemplar ja seifi lukukood antakse pitseeritud ümbrikus riigisaladuse kaitse juhendis määratud isikule, kes hoiab neid eraldi seifis.

(2) Seifi võtit ja lukukoodi võib hoida panga seifis.

(3) Muud seifiluku koodi ülestähendused on keelatud.

§ 79. Piiratud tasemel salastatud teabekandja säilitamiseks kasutatava kapi või sahtli võti

Piiratud tasemel salastatud teabekandja säilitamiseks kasutatava kapi või sahtli võtit tuleb hoida nii, et see oleks kaitstud kõrvaliste isikute kätte sattumise eest.

5. jagu
Salastatud teabekandja reprodutseerimine ja sellest väljavõtte tegemine

§ 80. Reprodutseerimise põhimõtted

(1) Töötlev üksus peab välistama salastatud teabekandja kontrollimatu reprodutseerimise ja sellest väljavõtte tegemise.

(2) Salajasel ja täiesti salajasel tasemel salastatud teabekandja reprodutseerimine ja sellest väljavõtte tegemine teabekandja koostanud töötleva üksuse kirjaliku nõusolekuta on keelatud. Lubatud on nõusolekuta reprodutseerida salastatud teavet töötleva üksuse töötlussüsteemis kasutamiseks.

(2[1]) Lõike 2 esimeses lauses sätestatud keeldu ei kohaldata teabekandja reprodutseerimisel ja sellest väljavõtte tegemisel, kui see sisaldab:
1) välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile edastatud salajasel tasemel salastatud riigisaladust;
2) salajasel tasemel salastatud välisteavet, kui välislepingutest ei tulene teisiti.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(3) Salajasel ja täiesti salajasel tasemel teabekandjat võib reprodutseerida ja sellest väljavõtte teha ainult registripidaja.

(4) Reprodutseerimise käigus reprodutseerimisvahendis jäädvustunud teavet tuleb kaitsta ebaseadusliku juurdepääsu eest.

§ 81. Reprodutseerimisseade

(1) Konfidentsiaalsel, salajasel ja täiesti salajasel tasemel salastatud teabekandja reprodutseerimise seade peab asuma turvaalal ning töötlev üksus peab tagama, et nendele reprodutseerimisseadmetele ei pääse juurde kõrvalised isikud. Salastatud teabekandja reprodutseerimiseks ja väljavõtte tegemiseks tuleb kasutada ainult selleks ettenähtud reprodutseerimisseadmeid.

(2) Piiratud tasemel salastatud teabekandja reprodutseerimine ja sellest väljavõtte tegemine on lubatud administratiivalal selleks ettenähtud reprodutseerimisseadmega.

6. jagu
Salastatud teabekandja hävitamine

§ 82. Salastatud teabekandja hävitamise põhimõtted

(1) Konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandja hävitamise seade peab asuma turvaalal. Turvaala kooskõlastava asutuse loal võib salastatud teabekandja hävitamise seade asuda administratiivalal.

[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(2) Kasutuskõlbmatuks muutunud salastatud teabekandja tuleb hävitada esimesel võimalusel, välja arvatud siis, kui seda on vaja säilitada eriotstarbeks.

§ 83. Salastatud teabekandja hävitamine

(1) Konfidentsiaalsel ja kõrgemal tasemel salastatud paberkandja hävitamiseks kasutatav paberipurustaja peab paberi purustama tükkideks, mis ei tohi olla suuremad kui 2 x 15 mm.

(2) Piiratud tasemel salastatud paberkandja hävitamiseks kasutatav paberipurustaja peab paberi purustama tükkideks, mis ei tohi olla suuremad kui 4 x 40 mm.

(3) Teisaldatava salvestuskandja hävitamise seadmed tuleb kooskõlastada Välisluureametiga.

(4) Lõigetes 1–3 nimetamata seadmeid võib kasutada salastatud teabekandja hävitamiseks vastavalt Kaitsepolitseiameti, Kaitseväe või Välisluureameti nõusolekul.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

§ 84. Salastatud teabekandja hävitamine juriidiliste isikute poolt

(1) Eraõiguslikud juriidilised isikud, kelle valduses on salastatud teave, edastavad hävitamisele kuuluva konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandja, sealhulgas originaali, koopia ja väljavõtte, hävitamiseks salastatud teabekandja koostanud või riigisaladuse töötlemisloa taotlemist toetanud asutusele.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(2) Kaitsepolitseiameti kirjalikul loal võib juriidiline isik hävitada lõikes 1 nimetatud salastatud teabekandja ka iseseisvalt, järgides käesolevas määruses kehtestatud nõudeid.

§ 85. Salastatud teabekandjat hävitavad füüsilised isikud

(1) Konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandja hävitamises peab osalema vähemalt kaks isikut, kes allkirjastavad salastatud teabekandja hävitamise akti.

(2) Hävitamises osalevatel isikutel peab olema vastaval tasemel riigisaladusele juurdepääsu õigus.

§ 86. Salastatud teabekandja hävitamise akt

(1) Salastatud teabekandja hävitamisel koostatakse salastatud teabekandja hävitamise akt.

(2) Salastatud teabekandja hävitamise aktis peavad olema märgitud:
1) salastatud teabekandjat identifitseerivad andmed;
2) teabekandja hävitanud isikute andmed;
3) hävitamismeetod.

(3) Salastatud teabekandja hävitamise akte säilitatakse turvaalal vähemalt viis aastat.

(4) Salastatud teabekandja hävitamise akti koostamata võib hävitada konfidentsiaalsel ja madalamal tasemel salastatud teabekandja registreerimata koopia.

7. jagu
Salastatud teabekandja edastamine

1. jaotis
Salastatud teabekandja edastamise üldpõhimõtted

§ 87. Vastuvõtja õigus juurde pääseda asjakohase taseme salastatud teabele

Riigisaladuse valdaja peab enne salastatud teabekandja edastamist olema veendunud, et salastatud teabekandja vastuvõtjal on asjakohasel tasemel salastatud teabele juurdepääsu õigus.

§ 88. Salastatud teabekandja edastamise pakend

(1) Salastatud teabekandja edastamiseks tuleb salastatud teabekandja panna läbipaistmatusse topeltpakendisse.

(2) Salastatud teabekandja peab olema pakendatud turvaliselt viisil, mis võimaldab tagantjärele tuvastada pakendi avamist. Vajaduse korral peab rakendama lisameetmeid pakendi sisu kaitsmiseks õigustamata isikute juurdepääsu eest.

(3) Välispakendile märgitakse saaja töötleva üksuse nimi, pakendis sisalduvate teabekandjate registreerimise numbrid ja vajaduse korral ka aadress.

(4) Sisepakendile märgitakse adressaadiks vastuvõtva töötleva üksuse salastatud teabekandjate register, samuti selles oleva teabekandja salastamistase, registreerimisnumber ja ühikute arv.

§ 89. Edastamise korraldamine

(1) Salastatud teabekandja edastamisel lepivad teabekandja edastaja ning saaja teabekandja edastamises kokku, järgides käesolevas määruses sätestatud nõudeid.

(2) Kui salastatud teabekandja edastamise kohta kehtestatud nõudeid ei ole töötleval üksusel võimalik järgida, peab ta pöörduma salastatud teabekandja edastamise korraldamiseks Kaitsepolitseiameti või Kaitseväe poole. [RT I, 19.08.2014, 17- jõust. 22.08.2014]

§ 90. Edastamisviis

(1) Salastatud teabekandja tuleb edastada viisil, mis tagab teadmisvajaduse põhimõtte arvestamise.

(2) Salastatud teabekandja edastatakse viivitamata. Salastatud teabekandja edastamiseks tuleb valida võimalikult lühike teekond ja ohutu viis.

(3) Kuller peab salastatud teabekandjat kuni üleandmiseni hoidma kogu aeg enda otseses valduses.

(4) Kui konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandjat ei ole võimalik kohe edastada, tagastatakse see saatja registripidajale või riigisaladuse kaitset korraldavale isikule.

(5) Piiratud tasemel salastatud teabekandjat võib edastada posti teel väljastusteatega tähtsaadetisena. Väljastusteadet säilitatakse registri juures.

§ 91. Kulleri õigus juurde pääseda salastatud teabele

Konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandja edastamiseks peab kulleril olema asjakohasel tasemel salastatud teabele juurdepääsu õigus.

§ 92. Salastatud teabekandja väljaviimine turvaalalt

Konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandja võib turvaalalt välja viia ainult töötleva üksuse juhi, registripidaja või töötleva üksuse riigisaladuse kaitse juhendis määratud muu isiku loal transportimiseks mõeldud lukustatavas kotis või kastis või pitseeritud diplomaatilise posti kotis.

§ 93. Salastatud teabekandja üleandmis-vastuvõtmisakt

(1) Salastatud teabekandja edastamise kohta koostab edastaja üleandmis-vastuvõtmisakti. Piiratud tasemel salastatud teabekandja edastamise kohta ei pea akti koostama.

(2) Üleandmis-vastuvõtmisakti peab olema märgitud:
1) teabekandja koostamise kuupäev, registreerimise number, kõrgeim salastatuse tase ning edastatavate ühikute arv. Üleandmis-vastuvõtmisakti ei tohi märkida pakendis sisalduva salastatud teabekandja pealkirja ega muud viidet teabekandja sisule;
2) adressaadiks oleva töötleva üksuse nimi ja aadress;
3) vastuvõtja nimi ja allkiri;
4) üleandja nimi ja allkiri.

(3) Vastuvõtja allkirjastab üleandmis-vastuvõtmisakti pärast edastatud pakendil ja aktis olevate kirjete võrdlemist.

(4) Üleandmis-vastuvõtmisakti säilitatakse registri juures turvaalal vähemalt viis aastat.

(5) Ühes ja samas üleandmis-vastuvõtmisaktis võib kajastada mitme salastatud teabekandja edastamist.

§ 94. Salastatud teabekandja vastuvõtja kohustused

(1) Salastatud teabekandja vastuvõtmisel kontrollitakse, kas saadetis on terviklik, kinnine ja avamisjälgedeta.

(2) Avatud saadetise või avamisjälgedega saadetise või sellise kahtluse korral peab sellest kohe teavitama registripidajat või muud riigisaladuse kaitse juhendis sätestatud isikut.

(3) Pärast välispakendi avamist tuleb sisepakend edastada viivitamata registreerimiseks registripidajale, kes edastab selle riigisaladuse kaitse juhendis sätestatud korras.

(4) Registripidaja peab kontrollima, kas teabekandjad ja neis sisalduv vastavad märgitud ühikute arvule.

2. jaotis
Salastatud teabekandja edastamine ühelt turvaalalt teisele administratiivala kaudu

§ 95. Administratiivala kaudu edastavad isikud

(1) Salastatud teabekandjat võib administratiivala kaudu edastada isiklikult, registripidaja või kulleriga.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(2) [Kehtetu -RT I, 14.01.2011, 6- jõust. 17.01.2011]

§ 96. Edastamise üldnõuete välistamine administratiivala kaudu edastamisel

Teabekandja edastamisele ühelt turvaalalt teisele ei kohaldata § 88 ja 92.

3. jaotis
Salastatud teabekandja edastamine avaliku ruumi kaudu

§ 97. Edastamine kahe füüsilise isiku poolt

Salajasel ja kõrgemal tasemel salastatud teabekandjat edastavad kaks füüsilist isikut. Kaitsepolitseiameti, Kaitseväe, riigi julgeoleku volitatud esindaja või Välisluureameti loal võib edastada ka üks isik.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

§ 98. Sõiduki kasutamine avaliku ruumi kaudu edastamisel

(1) Salajasel ja kõrgemal taseme salastatud teabekandjat edastatakse üldjuhul autoga.

(2) Auto aknad hoitakse suletud ja uksed lukustatud ning autojuht peab olema edastamist korraldava töötleva üksusega töö- või teenistussuhtes.

(3) Paragrahvis 99 nimetatud isikud ei või teabekandjat edastades samal ajal juhtida autot.

§ 99. Relva kandmine avaliku ruumi kaudu edastamisel

Täiesti salajasel tasemel salastatud teabekandjat edastav kuller peab kandma sõjaväe- või teenistusrelva või temaga peab olema kaasas sõjaväe- või teenistusrelva kandev isik.

4. jaotis
Salastatud teabekandja edastamine välismaale, välismaal ja välismaalt

§ 100. Välismaale, välismaal ja välismaalt kulleriga edastamine

(1) Välismaale, välismaal ja välismaalt edastatakse konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandja diplomaatilise või sõjalise kulleriga, kellel on asjakohasel tasemel salastatud teabele juurdepääsu õigus.

(2) Vastavalt Kaitsepolitseiamet, Kaitsevägi, riigi julgeoleku volitatud esindaja või Välisluureamet võib anda kirjaliku loa lõikes 1 nimetatud teabekandjate edastamiseks diplomaatilise või sõjalise kullerita juhul, kui kulleri kasutamine tooks kaasa ebasoovitava viivituse või kui teistsuguse edastamise vajadus on tingitud objektiivsest olukorrast.
[RT I, 19.08.2014, 17- jõust. 22.08.2014]

(2^1) Kui riigisaladust sisaldavat teabekandjat soovib diplomaatilise või sõjalise kullerita edastada julgeolekuasutus, annab selleks kirjaliku loa teabekandjaid edastava julgeolekuasutuse juht või tema volitatud isik.

[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(3) Lõikes 2 nimetatud luba peab sisaldama nõudeid, mida peab saadetise edastamisel täitma, eelkõige teekonna ja edastamiseks kasutatavate transpordivahendite kohta.

§ 101. Kuller välismaale, välismaal ja välismaalt edastamisel

(1) Välismaale, välismaal ja välismaalt edastamiseks peab kulleril olema diplomaatilise kulleri tunnistus, mille väljastab Välisministeerium, või diplomaatiline puutumatus.

(2) Sõjaliste missioonide piirkonnas edastamiseks peab kulleril olema sõjalise kulleri tunnistus, mille väljastab Kaitseministeerium.

8. jagu
Salastatud teabe elektrooniline töötlemine

[RT I, 26.10.2016, 2- jõust. 29.10.2016]

§ 102. Elektrooniline töötlemine
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

Salastatud teavet võib töödelda elektroonilise teabeturbe nõuetele vastavas töötlussüsteemis, millel on asjakohasel tasemel salastatud teabe töötlemiseks Välisluureameti poolt antud vastavussertifikaat või ajutine kasutusluba (edaspidi *akrediteeritud süsteem*) ja töötlemise ajal viibitakse sõltuvalt edastatavast teabest kas administratiiv- või turvaalal, välja arvatud §-s 103 sätestatud juhul.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

§ 103. Elektroonilise töötlemise erandid
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(1) Möödapääsmatu vajaduse korral võib piiratud tasemel salastatud teabe operatiivseks edastamiseks või vastuvõtmiseks töödelda teavet avalikus ruumis, kui kasutatakse avalikus ruumis töötlemiseks ette nähtud akrediteeritud süsteemi.

(2) Kui konfidentsiaalsel või kõrgemal tasemel salastatud riigisaladuse või konfidentsiaalsel või salajasel tasemel salastatud välisteabe operatiivne edastamine on vajalik riigi julgeolekut, põhiseaduslikku korda või isikute elu, tervist või vara ähvardava vahetu ohu ennetamiseks või tõrjumiseks, võib seda edastada ja vastu võtta, kui kasutatakse vähemalt piiratud tasemel salastatud teabe töötlemiseks akrediteeritud süsteemi. Teabe edastaja ja vastuvõtja peavad iga kord sellest viivitamata teavitama oma töötleva üksuse riigisaladuse kaitset korraldavat isikut.

(3) Kui teabe edastaja või vastuvõtja viibib lõikes 1 või 2 sätestatud juhul avalikus ruumis, peab ta:
1) enne teabe suulist edastamist teavitama teist poolt oma viibimisest avalikus ruumis;
2) rakendama kõiki vajalikke meetmeid edastatava teabe kaitsmiseks avalikuks tuleku ning juurdepääsuõiguseta või teadmisvajaduseta isikute juurdepääsu eest.

(4) Kui § 6 lõike 1 punktides 2–4 ja lõikes 3 nimetatud riigisaladuse või selle sisule vastava salastatud välisteabe operatiivne edastamata jätmine tooks kaasa jälitustoimingu nurjumise või seaks ohtu selles osalevad isikud, võib selle edastamise ja vastuvõtmise ajal viibida avalikus ruumis ning kasutada edastamiseks ja vastuvõtmiseks akrediteerimata süsteemi.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

9. jagu
Elektrooniline teabeturve

§ 104. Mõisted

Käesolevas jaos kasutatakse mõisteid järgmises tähenduses:
1) elektrooniline teabeturve – teabe käideldavuse, salajasuse ja terviklikkuse tagamine salastatud teabe töötlussüsteemides;
2) töötlussüsteemi akrediteerimine – töötlussüsteemi elektroonilise teabeturbe nõuetele vastavuse hindamine;
3) käideldavus – teabe kasutamise ja teabele juurdepääsu võimalus volitatud isiku nõudel;
4) salajasus – teabe volitamata isikutele mittekättesaadavus või mittearusaadavus;
5) terviklikkus – teabe omadus olla volitamata isikute poolt muutmata, täiendamata või hävitamata;
6) oht – teabe käideldavuse, salajasuse või terviklikkuse potentsiaalne kahjustumine;
7) turvarike – olukord, kus teave või selle kaitsmist toetavad süsteemitoimingud ja -vahendid kaotasid või võisid kaotada varguse, sabotaaži, terrorismiaktide, muu lubamatu tegevuse või turvaaukude tõttu salajasuse, terviklikkuse või käideldavuse (sealhulgas teabe kadumine, volitamata isikutele teatavakssaamine, volitamata isikute poolt muutmine või hävitamine või rünne süsteemi suhtes);

8) turvarisk – turvarikke esinemise tõenäosus;
9) riskihaldus – vara, teabe, ohu, turvarikke ja turvariski analüüs, mille põhjal määratakse kindlaks teabe ja selle kaitsmist toetavate süsteemitoimingute ja -vahendite turvameetmed. Riskihaldus hõlmab süsteemi turvameetmete planeerimist, korraldamist, kasutamist ja kontrollimist, selleks et vältida turvariski väljumist vastuvõetavatest piiridest ja turvarikkeid;
10) haavatavuse analüüs – süsteemi üksikasjalik kontrollimine, et selgitada välja süsteemi turvaaugud, ohud süsteemis töödeldava teabe salajasusele, terviklikkusele ja käideldavusele ning süsteemi vastuvõtlikkus mis tahes ründele või ohule;
11) töötlussüsteemi turvanõuete loetelu – süsteemi kohustuslike turvanõuete loetelu, mis sätestab, kuidas saavutada süsteemi piisav turvalisus ning kuidas tagada ja kontrollida teabe turvalisust süsteemis;
12) töötlussüsteemi turvanõuete rakendamise juhend – dokument, mis kirjeldab detailselt süsteemi turvanõuete loetelus ettenähtud turvanõuete täitmise korda ja iga konkreetse töötaja või muu isiku ülesandeid teabe turvalisuse tagamisel;
13) väline turvakeskkond – süsteemi paiknemiskohta ümbritsev keskkond, sealhulgas hoone või ala, milles toimuvad sündmused võivad mõjutada süsteemi turvalisust;
14) sisemine turvakeskkond – välise turvakeskkonnaga piirnev ruum või ala, kus paiknevad süsteemi komponendid või kus neid kasutatakse;
15) elektrooniline turvakeskkond – piirdub süsteemi komponentidega, mille abil teavet elektrooniliselt töödeldakse ning mille kaitseks süsteemi käitav personal rakendab elektroonilisi turvameetmeid.

§ 105. Elektroonilise teabeturbe põhimõtted

(1) Käesolevas osas sätestatakse elektroonilise teabeturbe nõuded salastatud teabe kaitseks selle elektroonilisel töötlemisel.

(2) [Kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

(3) Salastatud teavet on lubatud elektrooniliselt töödelda ainult sisemises turvakeskkonnas paiknevate arvutite ja kohtvõrkude abil, välja arvatud 8. jaos sätestatud tingimustel ja korras.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(3^1) Loa piiratud tasemel salastatud teabe elektrooniliseks töötlemiseks avalikus ruumis annab Välisluureamet töötlussüsteemi akrediteerimise käigus.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(4) Töötlusseadme, milles töötlemiseks lubatud kõrgeim teabe salastatuse tase on piiratud, võib viia väljapoole sisemist turvakeskkonda, kui:
1) salastatud teave on krüpteeritud nõuetele vastavate krüptovahenditega;
2) töötlusseadmel ei ole märgistust, mis viitaks töödeldava salastatud teabe salastatuse tasemele.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(5) Elektroonilise teabeturbe tagamisel salastatud välisteabe kaitseks võetakse täiendavalt arvesse salastatud välisteabe avaldaja poolt ettenähtud nõudeid.

(6) Elektroonilise teabeturbe tagamisel arvestatakse eelkõige järgmisi turvapõhimõtteid:
1) kasutada võib üksnes funktsioone, protokolle või teenuseid, mis on vajalikud teabe töötlemiseks või selle turvalisuse tagamiseks – minimaalsuse põhimõte;
2) katkematult peab toimuma süsteemi turvariskide ohjamine, sealhulgas vältimine, vähendamine, kõrvalejuhtimine ja lubatav aktsepteerimine – turvariskide pideva haldamise põhimõte – ja süsteemi turvalisuse regulaarne kontrollimine;
3) süsteemi kasutajatel ja administraatoritel on ainult tööülesannete täitmiseks vajalikud kasutajaõigused – privileegide piiratuse põhimõte;
4) eeldatakse kõigi süsteemiga ühendatud teiste süsteemide ebausaldusväärsust ning nendega teabe vahetamisel peab rakendama piisavaid turvameetmeid – isekaitsvate sõlmede kasutamise põhimõte;
5) ühe kasutatava turvameetme rikke korral ei tohi süsteem muutuda ebaturvaliseks – sügavuti kaitse põhimõte.

§ 106. Töötlussüsteemile esitatavad nõuded

(1) Salastatud teabe töötlussüsteemis peab olema tagatud salastatud teabe käideldavus, salajasus ja terviklikkus.

(2) Salastatud teabe töötlussüsteem peab võimaldama:
1) tuvastada ja registreerida isikud, kes omasid või võisid omada juurdepääsu salastatud teabe kaitsmist toetavatele süsteemitoimingutele ja -vahenditele;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
2) eristada süsteemi kasutajaid salastatud teabele juurdepääsu õiguse põhjal;
3) juurdepääsu teabele ja selle kaitsmist toetavatele süsteemitoimingutele ja -vahenditele üksnes juurdepääsuõiguse ja põhjendatud teadmisvajaduse olemasolul;

4) kontrollida teabe ning selle kaitsmist toetavate süsteemitoimingute ja -vahendite salajasust, terviklikkust, käideldavust, samuti nende päritolu, usaldatavust ja ühendusi;
5) saavutada olukorra, kus elektroonilise teabeturbe kaitsemehhanismid toimivad nõuetekohaselt süsteemi kogu kasutusaja jooksul;
6) ära hoida ja kõrvaldada turvarikkeid ning vältida või vähendada nende tekkimisega kaasnevat kahju;
7) käsitleda turvarikkeid, mille käigus määratakse kindlaks ja registreeritakse süsteemile või selle osale avaldunud oht ja selle tagajärjel teabele tekkinud kahju ning selle kõrvaldamiseks võetud meetmed.

(3) Süsteemi kohta käiv teave dokumenteeritakse süsteemi turvanõuete loetelus ja süsteemi turvanõuete rakendamise juhendis.

(4) Töötlev üksus teostab süsteemi suhtes pidevat riskihaldust.

§ 107. Süsteemi turvanõuete loetelu

(1) Süsteemi turvanõuete loetelus esitatakse:
1) süsteemi tehniline kirjeldus;
2) ülevaade süsteemi riskianalüüsi tulemustest;
3) süsteemile esitatavate turvanõuete kirjeldus;
4) süsteemis rakendatavate turvameetmete loetelu;
5) süsteemi turvalisuse korraldamise kirjeldus.

(2) Süsteemi turvanõuete loetelu töötab välja töötlev üksus. Enne salastatud teabe töötlemiseks uue süsteemi ehitamist või kasutusele võtmist kooskõlastab töötlev üksus loetelu Välisluureametiga.

(3) Süsteemi turvanõuete loetelu täpsustatakse süsteemi ehitamise ja kasutamise käigus, juhul kui toimuvad muudatused, näiteks kui muutub süsteemi kasutusotstarve, struktuur, ilmnevad uued olulised ohud või muutub süsteemis töödeldava salastatud teabe tase. Süsteemi turvanõuete loetelu muudatused kooskõlastab töötlev üksus Välisluureametiga.

§ 108. Süsteemi turvanõuete rakendamise juhend

(1) Süsteemi turvanõuete rakendamise juhendis esitatakse:
1) süsteemi turvalisuse eest vastutavate isikute ülesanded, õigused ja kohustused;
2) süsteemi kasutajad ning nende ülesanded, õigused ja kohustused;
3) süsteemi riist- ja tarkvara konfiguratsioonihalduse kirjeldus;
4) juhised salastatud teabe elektrooniliseks töötlemiseks;
5) süsteemis kasutatavate teabekandjate töötlemise kirjeldus;
6) süsteemi logifailide ülevaatamise ja intsidentide halduse kirjeldus.

(2) Süsteemi turvanõuete rakendamise juhendi töötab välja töötlev üksus, lähtudes süsteemi turvanõuete loetelust, ning kooskõlastab juhendi Välisluureametiga, enne kui süsteemis alustatakse salastatud teabe töötlemist.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

(3) Süsteemi turvanõuete rakendamise juhendit täpsustatakse süsteemi ekspluateerimise käigus, juhul kui toimuvad muudatused, näiteks kui muutub süsteemi kasutusotstarve, struktuur, ilmnevad uued olulised ohud või muutub süsteemis töödeldava salastatud teabe tase. Süsteemi turvanõuete rakendamise juhendi muudatused kooskõlastatakse Välisluureametiga.

§ 109. Süsteemi akrediteerimine

(1) Süsteemi akrediteerimise eesmärk on saada piisav veendumus, et süsteem vastab elektroonilise teabeturbe tagamiseks kehtestatud nõuetele.

(2) Süsteemi akrediteerimisel lähtub Välisluureamet:
1) süsteemi füüsilistest turvameetmetest;
2) süsteemiga seotud turvariskidest;
3) süsteemi turvanõuete loetelust;
4) süsteemi turvanõuete rakendamise juhendist;
5) süsteemi asukoha kiirgusturbe tsoneerimise tulemustest;
6) teabest elektroonilise teabeturbe nõuete täitmise kohta töötleva üksuse poolt.

(3) Välisluureamet algatab süsteemi akrediteerimise töötleva üksuse taotlusel või omal algatusel. Töötlev üksus lisab süsteemi akrediteerimise taotlusele süsteemi turvanõuete loetelu ja turvanõuete rakendamise juhendi. Ülejäänud lõikes 2 nimetatud teabe esitab töötlev üksus Välisluureameti nõudmisel.

(4) Akrediteerimise tulemusena antakse töötlevale üksusele vastavussertifikaat Välisluureameti peadirektori käskkirjaga.

(5) Süsteemile akrediteerimise tulemusena antav ajutine kasutusluba antakse Välisluureameti peadirektori käskkirjaga.

(6) Välisluureamet keeldub süsteemile vastavussertifikaati või ajutist kasutusluba väljastamast ja keelab selle kasutamise salastatud teabe töötlemiseks, kui süsteem ei vasta elektroonilise teabeturbe nõuetele. Vastav otsus tehakse Välisluureameti peadirektori käskkirjaga.

§ 110. Teabe andmise kohustus

Välisluureameti nõudel on töötlev üksus kohustatud viivitamata andma, sealhulgas kirjalikus vormis, teavet tema valduses oleva süsteemi ja elektroonilise teabeturbega seotud asjaolude kohta ning tagama Välisluureametile tööajal pideva ning puhkepäevadel ja riiklikel pühadel eelnevalt kokkulepitud ajal juurdepääsu süsteemi osadele, sõltumata nende paiknemiskohast.

§ 111. Vastavussertifikaadi ja ajutise kasutusloa kehtivuse pikendamise kord

(1) Vastavussertifikaadi pikendamiseks esitab töötlev üksus Välisluureametile taotluse vähemalt kaks kuud enne vastavussertifikaadi kehtivuse lõppemist.

(2) Ajutise kasutusloa kehtivust võib Välisluureamet pikendada omal algatusel ja töötleva üksuse taotluse alusel.

(3) Vastavussertifikaadi ja ajutise kasutusloa pikendamisele kohaldatakse süsteemi akrediteerimise sätteid.

§ 112. Vastavussertifikaadi ja ajutise kasutusloa kehtetuks tunnistamine

(1) Välisluureamet tunnistab vastavussertifikaadi või ajutise kasutusloa kehtetuks:
1) töötleva üksuse taotluse alusel;
2) kui töötlev üksus ei ole täitnud Välisluureameti ettekirjutust elektroonilise teabeturbe nõude rikkumise või rikkumise ohu kõrvaldamiseks;
3) ilmneb vastavussertifikaadi või ajutise kasutusloa andmisest keeldumise aluseks olev asjaolu.

(2) Vastavussertifikaat või ajutine kasutusluba tunnistatakse kehtetuks Välisluureameti peadirektori käskkirjaga.

(3) Vastavussertifikaadi või ajutise kasutusloa kehtetuks tunnistamine tehakse töötlevale üksusele teatavaks kirjalikult.

§ 113. Riigi julgeoleku volitatud esindaja teavitamine

Välisluureamet teavitab süsteemile vastavussertifikaadi või ajutise kasutusloa andmisest, vastavussertifikaadi kehtivuse pikendamisest või kehtetuks tunnistamisest riigi julgeoleku volitatud esindajat, kui süsteemis töödeldakse salastatud välisteavet.

10. jagu
Salastatud välisteabe kaitse

1. jaotis
Salastatud välisteabe töötlemine

§ 114. Salastatud välisteabe töötlemise põhimõtted

Salastatud välisteabe töötlemine toimub riigisaladuse töötlemisega samadel alustel ja korras, arvestades välislepingutest tulenevaid erisusi. Käesolevas jaos sätestatud töötlemisnõudeid ei kohaldata Välisluureametis arvele võetud krüptomaterjalile ning «Riigisaladuse ja salastatud välisteabe seaduse» § 52 lõikes 3 nimetatud teabele.

§ 115. Salastatud välisteavet sisaldavate teabekandjate arvestus

Salastatud välisteavet sisaldavate teabekandjate arvestust peetakse riigisaladuse arvestusest eraldi, nii et on tagatud registriandmetele ja teabekandjatele juurdepääsu piirang teadmisvajaduse ja juurdepääsuõiguse alusel. Registris tuleb arvestust pidada iga salastatud välisteabe avaldaja kohta eraldi.

§ 116. Riigi julgeoleku volitatud esindaja peetav salastatud välisteabe põhiregister

(1) Riigi julgeoleku volitatud esindaja peab salastatud välisteabe põhiregistrit, kus registreeritakse kõik riigile edastatud või riigis loodud salajasel ja kõrgemal salastatuse tasemel salastatud välisteabe kandjad ja kuhu

kogutakse andmed kõigi riigile edastatud või riigis loodud konfidentsiaalse tasemega salastatud välisteavet sisaldavate teabekandjate kohta.

(2) Töötlevad üksused, kes on riigi julgeoleku volitatud esindaja põhiregistri kasutajad, on kohustatud täitma §-s 51 sätestatud nõudeid.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

§ 117. Töötleva üksuse peetav salastatud välisteabe register

(1) Salastatud välisteavet valdav töötlev üksus on kohustatud sisse seadma salastatud välisteabe registri ja teavitama sellest eelnevalt kirjalikult riigi julgeoleku volitatud esindajat.

(2) Täiesti salajasel tasemel salastatud välisteabe ja erimärgistusega salastatud välisteabe töötlemiseks ning registri ja selle allregistri pidamiseks peab töötlev üksus saama riigi julgeoleku volitatud esindajalt kirjaliku nõusoleku. Riigi julgeoleku volitatud esindaja väljastab nõusoleku pärast kontrolli, mille käigus tuvastatakse, kas töötlemisnõuded on täidetud.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

§ 118. Salastatud välisteavet sisaldava teabekandja registreerimine

(1) Salastatud välisteavet valdav töötlev üksus on kohustatud tema valduses olevad salajase ja kõrgema salastatuse taseme ning erimärgistusega salastatud välisteavet sisaldavad teabekandjad registreerima lisaks töötleva üksuse registrile riigi julgeoleku volitatud esindaja poolt peetavas põhiregistris esimesel võimalusel, kuid mitte hiljem kui seitse tööpäeva pärast salastatud teabekandja loomist või töötlevasse üksusesse saabumist.

(2) Konfidentsiaalsel tasemel salastatud välisteavet sisaldavate teabekandjate kohta peab teavet valdav töötlev üksus edastama riigi julgeoleku volitatud esindajale andmed ühe kuu jooksul pärast salastatud teabekandja loomist või töötlevasse üksusesse saabumist.

(3) Töötlev üksus ei pea riigi julgeoleku volitatud esindaja poolt peetavas põhiregistris registreerima neid teabekandjaid, mille on talle edastanud riigi julgeoleku volitatud esindaja või töötlev üksus, kes on riigi julgeoleku volitatud esindaja põhiregistri kasutaja.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(4) Salastatud välisteavet valdav töötlev üksus on kohustatud kandma riigi julgeoleku volitatud esindaja antud registreerimisnumbri igale salajase ja kõrgema salastatuse taseme ning erimärgistusega salastatud välisteavet sisaldavale teabekandjale.

§ 119. Salastatud välisteavet sisaldava teabekandja edastamine

(1) Täiesti salajasel tasemel salastatud välisteavet ja erimärgistusega salastatud välisteavet sisaldav teabekandja võetakse vastu ning edastatakse teistele töötlevatele üksustele ainult riigi julgeoleku volitatud esindaja kaudu, välja arvatud juhul, kui registrit pidavale töötlevale üksusele on selleks antud riigi julgeoleku volitatud esindaja kirjalik nõusolek.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(2) [Kehtetu -RT I, 14.01.2011, 6- jõust. 17.01.2011]

(3) Salastatud välisteavet sisaldava teabekandja võib edastada ainult sellisele töötlevale üksusele, kes on eelnevalt sisse seadnud salastatud välisteabe registri.

§ 120. Täiesti salajasel tasemel salastatud välisteavet ja erimärgistusega salastatud välisteavet sisaldava teabekandja reprodutseerimine ja hävitamine
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(1) Täiesti salajasel tasemel salastatud välisteavet ja erimärgistusega salastatud välisteavet sisaldavat teabekandjat reprodutseerib ja hävitab ainult riigi julgeoleku volitatud esindaja.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(2) Riigi julgeoleku volitatud esindaja võib anda riigiasutusele kirjaliku loa lõikes 1 nimetatud teabekandja reprodutseerimiseks või hävitamiseks.

§ 121. Täiesti salajasel tasemel salastatud välisteavet ja erimärgistusega salastatud välisteavet sisaldava teabekandja tagastamine
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(1) Täiesti salajasel tasemel salastatud välisteabe või erimärgistusega salastatud välisteabe registrit pidav töötlev üksus tagastab nimetatud teavet sisaldava teabekandja riigi julgeoleku volitatud esindajale kohe pärast teabekandja kasutamise vajaduse lõppemist.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(2) Juhul kui teabekandjat on vaja kasutada kauem kui üks aasta pärast teabekandja saamist, tuleb teabekandja pikem hoidmine registreerida riigi julgeoleku volitatud esindaja peetavas põhiregistris.

§ 122. Riigi julgeoleku volitatud esindaja kontroll

Riigi julgeoleku volitatud esindaja viib vähemalt korra kahe aasta jooksul läbi salastatud välisteavet valdavas töötlevas üksuses salastatud välisteabe kaitse tagamiseks rakendatavate turvameetmete ja nimetatud teavet töötlevate füüsiliste isikute juurdepääsu kontrolli. Täiesti salajasel tasemel salastatud välisteavet või erimärgistusega teavet valdavates asutustes viib riigi julgeoleku volitatud esindaja kontrolli läbi vähemalt iga kaheksateistkümne kuu järel.
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

2. jaotis
Salastatud välisteabele juurdepääsu sertifikaadi väljastamise, selle väljastamisest keeldumise, pikendamise ja kehtetuks tunnistamise, juurdepääsuõiguse andmise, sellest keeldumise ja selle pikendamise kord

§ 123. Juurdepääs salastatud välisteabele

(1) Salastatud välisteabele juurdepääsu sertifikaat (edaspidi *juurdepääsusertifikaat*) antakse juurdepääsuks salastatud välisteabele, kui välislepingus on juurdepääsusertifikaadi andmine vastava taseme salastatud välisteabele juurdepääsu õiguse saamiseks ette nähtud.

(2) Välislepinguga ettenähtud juhtudel väljastab riigi julgeoleku volitatud esindaja ka salastatud välisteabele juurdepääsuõiguse kinnituse (edaspidi *kinnitus*).

(3) «Riigisaladuse ja salastatud välisteabe seaduse» § 27 lõigetes 1 ja 2 nimetatud isikutel tekib juurdepääsuõigus Euroopa Liidu ja Põhja-Atlandi Lepingu Organisatsiooni piiratud tasemega salastatud teabele pärast §-s 130 nimetatud tutvustuse läbimist ja kohustuse allkirjastamist ning §-s 131 nimetatud teatise väljastamist.

(4) Lõikes 3 nimetamata füüsilisel isikul ja eraõiguslikul juriidilisel isikul tekib salastatud välisteabele juurdepääsu õigus või töötlemise õigus ainult juurdepääsusertifikaadi alusel.

§ 124. Juurdepääsusertifikaadi taseme vastavus riigisaladuse loa tasemele

Juurdepääsusertifikaati ei anta kõrgemal salastatuse tasemel, kui on füüsilise isiku või töötleva üksuse, kellele juurdepääsusertifikaati taotletakse, riigisaladusele juurdepääsu loa või töötlemisloa tase.

§ 125. Juurdepääsusertifikaadi kehtivus

(1) Juurdepääsusertifikaadi kehtivusaja otsustab riigi julgeoleku volitatud esindaja vastavalt taotluses märgitud soovitavale kehtivusperioodile, riigisaladusele juurdepääsu õiguse kehtivusele ja teadmisvajaduse põhjendatusele. Juurdepääsusertifikaat ei või kehtida kauem kui isiku õigus pääseda juurde riigisaladusele.

(2) Juhul kui isiku õigus pääseda juurde riigisaladusele lõpeb enne juurdepääsusertifikaadil märgitud kehtivusaja lõppu, kaotab juurdepääsusertifikaat kehtivuse.

(3) Kui juurdepääsusertifikaat kaotab kehtivuse varem kui sellele märgitud kehtivuse lõppkuupäeval, tuleb juurdepääsusertifikaat tagastada riigi julgeoleku volitatud esindajale.

§ 126. Juurdepääsusertifikaadi taotlemine füüsilisele isikule

Füüsilisele isikule juurdepääsusertifikaadi taotlemiseks peab juurdepääsusertifikaati taotlev töötlev üksus esitama riigi julgeoleku volitatud esindajale järgmised dokumendid:
1) kirjalik taotlus, milles märgitakse salastatud välisteabe avaldaja ja salastatuse tase, millele juurdepääsu taotletakse, taotletav juurdepääsusertifikaadi kehtivusaeg, samuti isiku nimi, isikukood, selle puudumisel sünniaeg, täpne sünnikoht, kodakondsus ja kontaktandmed;
2) isiku juurdepääsuloa või muu riigisaladusele juurdepääsu õigust kinnitava dokumendi koopia;
3) koopia isiku isikutunnistuse mõlemast küljest või passi isikuandmetega lehest.

§ 127. Piiratud tasemel salastatud välisteabele juurdepääsu õiguse taotlemine

(1) Piiratud tasemel salastatud välisteabele juurdepääsu õiguse taotlemiseks § 123 lõikes 3 nimetatud isikule esitab asutus või põhiseaduslik institutsioon riigi julgeoleku volitatud esindajale kirjaliku taotluse, milles on märgitud isiku nimi, isikukood ja ametikoht ning lisatud koopia dokumendist, millega isikule on antud piiratud tasemel riigisaladusele juurdepääsu õigus.

(2) Vajaduse korral väljastab riigi julgeoleku volitatud esindaja kinnituse ka piiratud tasemel salastatud välisteabele juurdepääsu õiguse tõendamiseks.

§ 128. Juurdepääsusertifikaadi taotlemine töötlemisloa alusel salastatud teavet töötlevale isikule

Juurdepääsusertifikaadi taotlemiseks töötlemisloa alusel salastatud teavet töötlevale isikule peab juurdepääsu andmist toetav asutus esitama riigi julgeoleku volitatud esindajale järgmised dokumendid:
1) töötleva üksuse kirjalik taotlus, milles nimetatakse salastatud välisteabe avaldaja ja salastatuse tase, millele juurdepääsu taotletakse, ning põhjendatakse isiku salastatud välisteabele juurdepääsu vajadust;
2) toetava asutuse kirjalik taotlus, milles nimetatakse salastatud välisteabe avaldaja ja salastatuse tase, millele juurdepääsu taotletakse, ning põhjendatakse isiku salastatud välisteabele juurdepääsu vajadust, välja arvatud juhul, kui toetavaks asutuseks on riigi julgeoleku volitatud esindaja;
3) töötlemisloa koopia;
4) riigisaladuse kaitse juhendi koopia;
5) koopia dokumendist, millega määratakse juriidilise isiku riigisaladuse kaitset korraldav isik ja tema nimi, samuti nende isikute nimekiri, kes hakkavad salastatud välisteavet töötlema, ning vajaduse korral dokumendid neile füüsilise isiku juurdepääsusertifikaadi taotlemiseks.

§ 129. Juurdepääsusertifikaadi andmise otsustamine taotluse alusel

(1) Kui juurdepääsusertifikaadi andmise taotlus või sellele lisatud dokumendid ei vasta nõuetele, annab riigi julgeoleku volitatud esindaja füüsilisele isikule juurdepääsusertifikaati taotlenud töötlevale üksusele või töötlevale üksusele juurdepääsusertifikaadi andmist toetanud asutusele või põhiseaduslikule institutsioonile kümne tööpäeva jooksul teada puudustest ning määrab tähtaja nende kõrvaldamiseks.

(2) Juurdepääsusertifikaadi andmise või sellest keeldumise otsustab riigi julgeoleku volitatud esindaja ühe kuu jooksul nõuetekohase taotluse saamisest. Põhjendatud vajaduse korral võib tähtaega pikendada, teavitades sellest taotlevat või toetavat asutust või põhiseaduslikku institutsiooni.

§ 130. Välisteabe kaitse nõuete tutvustamine

(1) Riigi julgeoleku volitatud esindaja või tema poolt volitatud asutus tutvustab füüsilisele isikule enne esmakordset piiratud tasemel salastatud välisteabele juurdepääsu õiguse või juurdepääsusertifikaadi andmist salastatud välisteabe kaitse aluseid. Vajadusel viib riigi julgeoleku volitatud esindaja tutvustamise läbi ka juurdepääsusertifikaadi või juurdepääsuõiguse korduval andmisel või kinnituse väljastamisel.

(2) Kui piiratud tasemel salastatud välisteabele juurdepääsu õigus või juurdepääsusertifikaat antakse töötlevale üksusele, tutvustakse salastatud välisteabe kaitse aluseid selle riigisaladuse kaitset korraldavale isikule.

(3) Juurdepääsuõiguse või juurdepääsusertifikaadi saavalt füüsiliselt isikult, töötleva üksuse puhul riigisaladuse kaitset korraldavalt isikult võtab riigi julgeoleku volitatud esindaja enne juurdepääsusertifikaadi üleandmist või teatise väljastamist allkirja kohustuse kohta hoida temale töö või teenistuse kaudu teatavaks saavat salastatud välisteavet.

§ 131. Juurdepääsusertifikaadi ja teatise edastamine

Riigi julgeoleku volitatud esindaja edastab juurdepääsusertifikaadi või teatise piiratud tasemel salastatud välisteabele juurdepääsu õiguse tekkimisest viie tööpäeva jooksul vastavalt juurdepääsu taotlenud töötlevale üksusele või juriidilise isiku juurdepääsu toetanud asutusele. Töötlevale üksusele, kelle juurdepääsuõiguse taotlust toetati, edastatakse juurdepääsusertifikaadi koopia.

§ 132. Juurdepääsusertifikaadi vormistamine

(1) Juurdepääsusertifikaadil peavad olema vähemalt järgmised andmed:
[RT I, 22.11.2016, 7- jõust. 01.01.2017]
1) väljaandmise kuupäev ja number;
2) juurdepääsusertifikaadi saanud füüsilise isiku ees- ja perekonnanimi, sünniaeg, sünnikoht või juriidilise isiku nimi, aadress ja registrikood;
3) salastatud välisteabe kõrgeim tase ja erikategooriad, millele lubatakse isiku juurdepääs;
4) juurdepääsusertifikaadi kehtivusaeg;
5) vajaduse korral selle ürituse nimetus, toimumise aeg ja koht, millel osalemiseks juurdepääsusertifikaati taotleti.

(2) Juurdepääsusertifikaat vormistatakse inglise ja eesti keeles.

§ 133. Kinnituse taotlemine ja vormistamine

(1) Kinnituse taotlemiseks esitab töötlev üksus taotluse, millele lisatakse dokumendid ürituse või sündmuse kohta, millel osalemiseks kinnitust taotletakse, ja riigi julgeoleku volitatud esindaja nõudmisel täiendavad dokumendid, kui see tuleneb välislepingust.

(2) Kinnituse vormistamisel järgitakse § 132 lõike 1 nõudeid.
[RT I, 22.11.2016, 7- jõust. 01.01.2017]

§ 134. Juurdepääsusertifikaadi kehtetuks tunnistamine

Juurdepääsusertifikaat tunnistatakse kehtetuks:
1) isiku teadmisvajaduse äralangemisel;
2) uue juurdepääsusertifikaadi väljastamisel enne eelmise juurdepääsusertifikaadi kehtivusaja lõppu;
3) juurdepääsusertifikaadile kantud isikuandmete muutumisel;
4) kui väljastatud juurdepääsusertifikaadi kehtimise ajal ilmneb mõni juurdepääsusertifikaadi väljastamist välistav asjaolu.

§ 135. Juurdepääsu- ja töötlemisloa, juurdepääsuõiguse ja -vajaduse lõppemisest teavitamine

Füüsilisele isikule salastatud välisteabele juurdepääsu õiguse andmist taotlenud töötlev üksus ja töötleva üksuse taotlust toetanud asutus või põhiseaduslik institutsioon teavitab viivitamata riigi julgeoleku volitatud esindajat juurdepääsuõiguse saanud isiku salastatud välisteabele juurdepääsu vajaduse või riigisaladusele juurdepääsu loa või õiguse või töötlemisloa lõppemisest.

§ 136. Julgeolekukontrolli teostamiseks pädeva asutuse teavitamine

Riigi julgeoleku volitatud esindaja teavitab viivitamata isiku suhtes julgeolekukontrolli teostamiseks pädevat asutust füüsilisele või juriidilisele isikule salastatud välisteabele juurdepääsu õiguse ja juurdepääsusertifikaadi andmisest, selle õiguse kehtetuks tunnistamisest või tühisuse tuvastamisest.

6. peatükk
NÕUSOLEKU, KINNITUSE, JUURDEPÄÄSULOA JA TÖÖTLEMISLOA NING NENDE KEHTIVUSE PIKENDAMISE TAOTLUSE, JUURDEPÄÄSULOA JA TÖÖTLEMISLOA TAOTLEJA JA PIKENDAJA ANKEEDI VORMIDE KEHTESTAMINE

§ 137. Riigisaladusele juurdepääsu loa vormid

(1) Füüsiline isik esitab riigisaladusele juurdepääsu loa (edaspidi *juurdepääsuluba*) lisas 1 toodud taotluse vormil.

(2) Füüsiline isik esitab juurdepääsuloa kehtivuse pikendamise lisas 2 toodud taotluse vormil.

(3) Füüsiline isik täidab juurdepääsuloa taotlemisel või juurdepääsuloa kehtivuse pikendamise taotlemisel juurdepääsuloa taotleja ja pikendaja ankeedi (lisa 3).
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

(4) [Kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

(5) Füüsiline isik täidab juurdepääsuloa ja selle kehtivuse pikendamise taotlemisel ankeedi lisana nõusoleku vormi (lisa 5).

(6) Füüsiline isik kinnitab juurdepääsuloa ja selle kehtivuse pikendamise taotlemisel, et ta on teadlik riigisaladuse kaitse nõuetest, vastutusest nende rikkumise eest ja kohustusest hoida temale teatavaks saavat riigisaladust (lisa 6).

(7) Üksnes piiratud taseme riigisaladusele juurdepääsu õigust taotlev või omav isik täidab lõikes 5 nimetatud nõusoleku vormi ja annab lõikes 6 nimetatud kinnituse.
[RT I, 14.01.2011, 6- jõust. 17.01.2011]

§ 138. Riigisaladuse töötlemisloa vormid

(1) Juriidiline isik esitab riigisaladuse töötlemisloa (edaspidi *töötlemisluba*) taotluse lisas 7 toodud vormil.

(2) Juriidiline isik esitab töötlemisloa kehtivuse pikendamise taotluse lisas 8 toodud vormil.

(3) Juriidiline isik täidab töötlemisloa taotlemisel töötlemisloa taotleja ankeedi (lisa 9).

(4) Juriidiline isik täidab töötlemisloa kehtivuse pikendamise taotlemisel töötlemisloa pikendaja ankeedi (lisa 10)

(5) Juriidiline isik täidab töötlemisloa ja selle kehtivuse pikendamise taotlemisel ankeedi lisana nõusoleku vormi (lisa 11).

(6) Juriidiline isik kinnitab töötlemisloa ja selle kehtivuse pikendamise taotlemisel, et ta on teadlik riigisaladuse kaitse nõuetest, vastutusest nende rikkumise eest ja kohustusest hoida temale teatavaks saavat riigisaladust (lisa 12).

(7) Lõikeid 1–6 kohaldatakse ka füüsilisest isikust ettevõtjale.

7. peatükk
MÄÄRUSE RAKENDAMINE

§ 139. Määruse jõustumine

(1) Määrus jõustub 1. jaanuaril 2008. a.

(2) Paragrahvi 8 lõike 1 punktid 4, 5, 7, 8 ja 11 jõustuvad 1. jaanuaril 2009. a, välja arvatud teabe osas, mis oli riigisaladuseks enne 1. jaanuari 2008. a.

(3) Paragrahvi 70 lõige 1 jõustub 1. jaanuaril 2009. a.

Lisa 1 Riigisaladusele juurdepääsu loa taotlus

Lisa 2 Riigisaladusele juurdepääsu loa kehtivuse pikendamise taotlus

Lisa 3 Füüsilise isiku täiesti salajase, salajase või konfidentsiaalse taseme riigisaladusele juurdepääsu loa taotleja ja juurdepääsuloa kehtivusaja pikendaja ankeet
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

Lisa 4 Füüsilise isiku täiesti salajase, salajase või konfidentsiaalse taseme riigisaladusele juurdepääsu loa pikendaja ankeet
[Kehtetu -RT I, 26.10.2016, 2- jõust. 29.10.2016]

Lisa 5 Füüsilise isiku nõusolek julgeolekukontrolli teostamiseks
[RT I, 26.10.2016, 2- jõust. 29.10.2016]

Lisa 6 Füüsilise isiku kinnitus hoida teatavaks saavat riigisaladust

Lisa 7 Riigisaladuse töötlemisloa taotlus

Lisa 8 Riigisaladuse töötlemisloa kehtivuse pikendamise taotlus

Lisa 9 Riigisaladuse töötlemisloa taotleja ankeet

Lisa 10 Riigisaladuse töötlemisloa pikendaja ankeet

Lisa 11 Juriidilise isiku riigisaladuse töötlemisloa või selle kehtivuse pikendamise taotleja kirjalik nõusolek

Lisa 12 Juriidilise isiku kinnitus hoida teatavaks saavat riigisaladust