

Väljaandja:
Akti liik:
Teksti liik:
Redaktsiooni jõustumise kp:
Redaktsiooni kehtivuse lõpp:
Avaldamismärge:

Vabariigi Valitsus
määrus
terviktekst
01.01.2024
Hetkel kehtiv
RT I, 29.12.2023, 12

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.
21.06.2018	RT I, 28.06.2018, 6	01.07.2018
02.08.2018	RT I, 07.08.2018, 2	10.08.2018
28.02.2019	RT I, 06.03.2019, 7	09.03.2019
04.10.2021	RT I, 06.10.2021, 1	09.10.2021
23.12.2021	RT I, 31.12.2021, 18	03.01.2022
26.08.2022	RT I, 27.08.2022, 1	01.09.2022, osaliselt 01.01.2023
25.05.2023	RT I, 31.05.2023, 3	05.06.2023
21.12.2023	RT I, 29.12.2023, 8	01.01.2024

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) [kehtetu -[RT I, 31.05.2023, 3](#)- jõust. 05.06.2023]

- 3) administratiivala – ala, millel on lubatud piiratud tasemel riigisaladuse või salastatud välisteabe ja seda sisaldava salastatud teabekandja töötlemine;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 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 veab salastatud teabekandjat;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 8) rahvusvaheline külastustaotlus – rahvusvahelise külastuse puhul vastuvõtva riigi asjaomasele asutusele esitatav taotlus, mis hõlmab juurdepääsu teise riigi või rahvusvahelise organisatsiooni salastatud teabele, kui see on välislepinguga ette nähtud.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 2¹. 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 tseremooniade (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;
- 7) välissuhtlemisasutuse loodud teave, mis käsitleb rahvusvahelisi suhteid, välisriiki või rahvusvahelist institutsiooni või nende esindajat, kui teabe sisu, selle edastamise viisi või allika avalikustamine kahjustaks oluliselt riigi julgeolekut. Selline teave salastatakse salajasel tasemel 50 aastaks.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2) Strateegilise kauba sisseveo, väljaveo, transiidi, sõjalise kaubaga seotud teenuse osutamise 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 osutamise ja strateegilise kauba lõppkasutuse kohta, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 50 aastaks;

2) strateegilise kauba komisjoni ülesannete täitmiseks koostatud teave strateegilise kauba sisseveo, väljaveo, transiidi, sõjalise kaubaga seotud teenuse osutamise ja strateegilise kauba lõppkasutuse kohta, milles analüüsitakse strateegilise kauba levikut ja sellega seotud ohtu julgeolekule. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;

3) strateegilise kauba komisjoni koostatud teave sõjalise kauba, välja arvatud massihävitusrelvadega seotud materjalide, rajatiste ja seadmete, sisseveo- või väljaveolitsentsi, transiidiloo või lõppkasutuse järelevalve dokumendi väljastamisest keeldumise kohta; samuti teave sellist keeldumist arutanud strateegilise kauba komisjoni koosolekul käsitletu kohta. See teave salastatakse piiratud tasemel 50 aastaks, välja arvatud juhul, kui selle avalikuks tulek ei kahjusta riigi julgeolekut ega kahjusta oluliselt välissuhtlemist;

4) strateegilise kauba komisjoni edastatav teave rahvusvahelistele kontrollsüsteemidele, välisriikidele ja Euroopa Liidule, mida kaitstakse avalikuks tuleku eest rahvusvaheliste tavade kohaselt või mille kaitsmises on kohtumisel või muul üritusel osalejate vahel kokku lepitud. Selline teave salastatakse salajasel tasemel 50 aastaks, välja arvatud juhul, kui osalejate kokkuleppel või rahvusvahelise tava kohaselt on määratud muu salastatuse tase või salastamistähtaeg.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 5. Riigikaitse riigisaladuse alaliigid

(1) Riigikaitse ettevalmistamist, juhtimist ja tegevust käsitleva teabe osas on riigisaladuseks:

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

1) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

1¹) [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 operatsiooniplaanimist ja operatsioonijuhtimist kajastav teave. See teave salastatakse salajasel tasemel 50 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

3¹) Kaitseväe sõjalise riigikaitse riigi territoriaalsel jaotusel põhinevat operatsiooniplaanimist ja operatsioonijuhtimist kajastav teave. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

4) Kaitseväe väeliigi, väejuhatuse, brigaadi ja Kaitseväe korralduse seaduse § 37 lõike 1 punktides 1, 2 ja 5 ning lõikes 2 nimetatud viisil teavet koguva kaitsevälisuse ülesannet või erioperatsioonide korraldamise ülesannet täitva üksuse operatsiooniplaanimist ja operatsioonijuhtimist kajastav teave. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

5) Kaitseväe sõjaaja üksuse operatsiooniplaanimist ja operatsioonijuhtimist kajastav teave, mida ei salastata punktide 3–4 alusel. See teave salastatakse piiratud tasemel 30 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

13) sõjaajal kasutatava elektroonilise side võrgu tehniline teave ja tööparameetrid, mille avalikuks tulek kahjustaks Eesti Vabariigi julgeolekut. See teave salastatakse § 22 lõike 1 punkti 17 alusel kehtestatud korras salajasel või madalamal tasemel 50 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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 alaliselt tegutseva struktuuriüksuse ning sõjaaja üksuse, välja arvatud üksuse ülema ametikoht, ja nende allüksuse koosseis ja komplekteeritus, ülesandeid ja teenistujate ülesandeid, eelarve kulude liigendust, eelarve täitmise aruandlust, eelarve planeerimist ja investeringuid kajastav teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 50 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 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 50 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 21) teave küberoperatsioonide korraldamiseks kasutatavate meetodite ja vahendite kohta, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 50 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 22) riigikaitse ühtseks planeerimiseks töödeldav riigikaitseülesannetega täidesaatva riigivõimu asutuse või asutuste tegevusi, võimeid ja vajadusi kajastav koondteave, välja arvatud teave, mille avalikuks tulek ei kahjusta riigi julgeolekut. See teave salastatakse salajasel tasemel kuni 50 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 23) riigikaitseülesandega täidesaatva riigivõimu asutuse riigikaitseks valmistumist, sealhulgas tegevusi, võimeid ja vajadusi kajastav teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel kuni 50 aastaks.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

- 1) mobilisatsiooniregistrisse kantud andmed kogumis. See teave salastatakse salajasel tasemel 30 aastaks;
- 2) [kehtetu -RT I, 28.06.2018, 6- jõust. 01.07.2018]
- 3) [kehtetu -RT I, 28.06.2018, 6- jõust. 01.07.2018]
- 4) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 5) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 6) Kaitseväe sõjaaja üksuste lahinguvõimudest kajastavad koondandmed, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 30 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 7) ühe Kaitseväe sõjaaja üksuse lahinguvõimudest kajastavad koondandmed, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(3) Mobilisatsiooni korraldamiseks vajalikku varu käsitleva teabe osas on riigisaladuseks teave mobilisatsiooni korraldamiseks vajaliku varu ja vahendite üldkoguste kohta. See teave salastatakse salajasel tasemel 30 aastaks.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(4) Kaitseväe ja Kaitseliidu sõjaväerelvi, lahingumoonna ja laskemoona käsitleva teabe osas on riigisaladuseks:
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 1) Kaitseväe ja Kaitseliidu sõjaväerelvade, lahingumoonna ja laskemoona koondandmeid ja -jaotust kajastav teave, välja arvatud teave, mille avaldamine on kohustuslik välislepingu alusel. See teave salastatakse salajasel tasemel 20 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 2) [kehtetu -RT I 2008, 55, 312- jõust. 01.01.2009]
- 3) mereväe relvasüsteemide taktikalised andmed. See teave salastatakse konfidentsiaalsel tasemel 10 aastaks.
[RT I, 27.08.2022, 1- jõust. 01.09.2022]

(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 30 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 3) õhuväe õhuseiresüsteemi koondparameetrid ja radarite võime parameetrid, mille avalikuks tulek võib kahjustada õhuseiret. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 4) radari elektroonilise sõjapidamise meetmete ja vahendite tehniline kirjeldus. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 5) radari elektroonilise sõjapidamise võime testi tulemused. See teave salastatakse salajasel tasemel 30 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 6) radari kasutatavad töörežiimid, filtreeritud alad ja sihtmärgi kriteeriumid. See teave salastatakse konfidentsiaalsel tasemel 30 aastaks;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 7) radari tegevus seisund ja hooldusajad üldise kaitsevalmiduse ajal. See teave salastatakse piiratud tasemel üheks aastaks;
[RT I, 26.10.2016, 2- jõust. 29.10.2016]
- 8) radari tegevus seisund 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 õhukaitse süsteemi koodnimetuse rakendamise ja kindlale süsteemile määramise kohta. See teave salastatakse piiratud tasemel 10 aastaks. Õhukaitse süsteemi koodnimetus ei ole riigisaladus;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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 kogutud ja töödeldud terviklik radariteave, mille avalikuks tulek võib kahjustada õhuseiresüsteemi. See teave salastatakse § 22 lõike 1 punkti 17 alusel kehtestatud korras salajasel või madalamal tasemel 15 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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) Riigikaitsete leiutisi ja uuringuid ning nende tulemusi käsitleva teabe osas on riigisaladuseks riigikaitsete 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) Kaitsevæeluurega tegeleva Kaitsevæe struktuuriüksuse kogutud ja sünteesitud teabe osas on riigisaladuseks:

1) sideluure vahenditega kogutud teave või selle põhjal sünteesitud teave, mille põhjal on võimalik tuvastada kogumisviisi. 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;

3¹) 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]

3²) 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 3–3² nimetatud 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) kaitsevæeluuret teostava Kaitsevæe struktuuriüksuse poolt koostatud ohuhinnangut käsitlev teave. See teave salastatakse salajasel tasemel 50 aastaks;

8) kaitsevæeluuret teostava Kaitsevæe struktuuriüksuse poolt julgeolekuasutuste korraldatud luure- ja vastuluureoperatsioonide käigus kogutud teave või selle alusel sünteesitud teave. See teave salastatakse salajasel tasemel 30 aastaks;

9) punktides 5 ja 6 nimetatud teave, mille lähteandmed on salastatud nendes punktides sätestatuga võrreldes kõrgemal tasemel või pikemaks tähtajaks. See teave salastatakse lähteandmete kõrgeimast salastatuse tasemest ja pikimast salastamistähtajast lähtudes;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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) alaliselt tegutseva struktuuriüksuse või sõjaaja üksuse või nende allüksuse ülesehitust, koosseisu, ameti- ja töökohti käsitlev teave, välja arvatud alaliselt tegutseva struktuuriüksuse või sõjaaja üksuse ülema ametikoht ja teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 50 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2) alaliselt tegutseva struktuuriüksuse või sõjaaja üksuse või nende allüksuse ja teenistujate ülesandeid käsitlev teave, välja arvatud teave, mille avalikustamine ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 50 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

3) alaliselt tegutseva struktuuriüksuse või sõjaaja üksuse või nende allüksuse teenistujate koondandmed, samuti andmed kaitseväeluure värbamisstatistika ja sellega seotud ametikohtade komplekteerimise ning täitvuse kohta. See teave salastatakse salajasel tasemel 50 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

4) alaliselt tegutseva struktuuriüksuse või sõjaaja üksuse või nende allüksuse eelarve kulude liigendus, eelarve täitmise aruandlus, eelarve planeerimist ja investeringuid kajastav teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 50 aastaks.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 kaitseväeluure teostava Kaitseväe struktuuriüksuse poolt 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 salajasele koostööle kaasatud isiku ja variisiku kohta. 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, 31.05.2023, 3- jõust. 05.06.2023]

6) andmed, millest nähtub Kaitseväe poolt teeseldud juriidilise isiku, tema struktuuriüksuse, organi või äriühingu filiaali seotus Kaitseväega. See teave salastatakse salajasel tasemel 50 aastaks.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 Kaitseväe militaargeograafia valdkonda käsitleva teabe osas on riigisaladuseks:

1) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

2) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

3) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

4) riigi sõjalist kaitsemist ja selle ettevalmistamist toetav militaargeograafiline teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 15 aastaks.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 6. Korrakaitse riigisaladuse alaliigid

(1) Jälitusasutuste poolt jälitustegevuse käigus kogutud teave 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) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

2¹) jällitusasutuse poolt „Karistusseadustiku“ 8., 15., 16. ja 22. peatükis sätestatud kuritegudes ning Kaitsepolitsei ameti uurimisalluvuses olevates kuritegudes jälitustoiminguga kogutud teave, kui selle avalikuks tulek võib kahjustada Eesti Vabariigi julgeolekut. 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 puutumatus jälitustoiminguga riivati; [RT I, 31.05.2023, 3- jõust. 05.06.2023]

3) jälitusasutuse poolt jälitustegevuses salajasele koostööle kaasatud isikult saadud ja variisiku poolt kogutud teave. See teave salastatakse piiratud tasemel 50 aastaks; [RT I, 31.05.2023, 3- jõust. 05.06.2023]

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) Jällitusasutuste 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]

(11) Politsei- ja Piirivalveameti isikukaitse üksuse kaitseoperatsioonide läbiviimist käsitlev teave, sealhulgas meetodeid, taktikat ja vahendeid käsitlev teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 25 aastaks või kuni isikukaitse osutamise vajaduse äralangemiseni või isikukaitse osutamise lõppemiseni.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(12) Politsei- ja Piirivalveameti eriüksuse relvastuse, laskemoona, erivahendite ja varustust käsitleva teabe osas on riigisaladuseks:

1) relvastuse, laskemoona, erivahendite ja muu varustuse koondandmeid, hoidmist ja jaotust kajastav teave. See teave salastatakse piiratud tasemel 25 aastaks;

2) teave eriüksuse relvastuse, laskemoona, erivahendite ja muu varustuse tehniliste andmete kohta, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 25 aastaks.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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 25 aastaks või kuni hoone või rajatise valdamise lõppemiseni;

[RT I, 06.03.2019, 7- jõust. 09.03.2019]

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, eelarve täitmise aruandlus, eelarve planeering ja investeeringud. See teave salastatakse salajasel tasemel 50 aastaks.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 teave 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 töötaja 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 varjatult 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 50 aastaks;

[RT I, 06.03.2019, 7- jõust. 09.03.2019]

2) julgeolekuasutuse ülesannete täitmisel analüüsitud ja sünteesitud teave, mis kajastab riigisiseseid või välismaiseid ohuallikaid. See teave salastatakse konfidentsiaalsel tasemel 50 aastaks;

[RT I, 06.03.2019, 7- jõust. 09.03.2019]

3) julgeolekuasutuse poolt koostatud ohuhinnangud, välja arvatud käesoleva lõike punktis 3¹ nimetatud ohuhinnangud. See teave salastatakse salajasel tasemel 50 aastaks;

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

3¹) 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) punktides 1–4 nimetatud teave, mille lähteandmed on salastatud nendes punktides sätestatuga võrreldes kõrgemal tasemel või pikemaks tähtjaks. See teave salastatakse lähteandmete kõrgeimast salastatuse tasemest ja pikimast salastamistähtjast lähtudes;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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 3¹ ja 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 tähtjaks.

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

(5¹) 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 50 aastaks;

[RT I, 06.03.2019, 7- jõust. 09.03.2019]

2) julgeolekuasutuse struktuuriüksuste ja teenistujate ülesanded, välja arvatud teave, mille avalikustamine ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse salajasel tasemel 50 aastaks;

[RT I, 06.03.2019, 7- jõust. 09.03.2019]

3) julgeolekuasutuse teenistujate koondandmed ja üksnes teabe varjatud kogumisega seonduvaid tööülesandeid täitvate teenistujate koosseis. See teave salastatakse salajasel tasemel 50 aastaks;

[RT I, 06.03.2019, 7- jõust. 09.03.2019]

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 välisuhtluse 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]

6¹) Siseministeeriumi ja Kaitseministeeriumi koostatud julgeolekuasutuste 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]

6²) julgeolekuasutuste 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]

(9¹) Lõike 9 punktides 3 ja 6–6² nimetatud teave, mille lähteandmed on salastatud nendes punktides sätestatuga võrreldes kõrgemal tasemel või pikemaks tähtjaks, salastatakse lähteandmete kõrgeimast salastatuse tasemest ja pikimast salastamistähtjast lähtudes. [RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 tähtjaks, kui register sisaldab vastava salastatuse taseme ja tähtjaga teavet. [RT I, 14.01.2011, 6- jõust. 17.01.2011]

§ 8. Infrastruktuuri ja teabe kaitse riigisaladuse allaliigid

(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 töötlevate üksuste 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, 31.05.2023, 3- jõust. 05.06.2023]

17) [kehtetu -RT I, 19.08.2014, 17- jõust. 22.08.2014]

18) Kaitseministeeriumi, Kaitseväe, Kaitseliidu, Kaitseressursside Ameti ja teiste Kaitseministeeriumi valitsemisalas töötlevate üksuste asutusesiseseks kasutamiseks mõeldud teabe töötlemiseks kasutatavate töötlussüsteemide, milles ei töödelda salastatud teavet, tehnilisi andmeid ja turvameetmeid kajastav teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel kuni töötlussüsteemi või selle osa kasutamise lõppemiseni, kuid mitte kauemaks kui 30 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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 võtmega 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]

25¹⁾ 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) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

27) välispiiride valvamiseks mõeldud 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, 27.08.2022, 1- jõust. 01.01.2023]

28) välispiiride valvamiseks mõeldud 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 30 aastaks või kasutamise lõppemiseni;

[RT I, 27.08.2022, 1- jõust. 01.01.2023]

29) välispiiride valvamiseks mõeldud seire- ja valvesüsteemide katvuspiirkondi kajastavate testide tulemused. See teave salastatakse piiratud tasemel 10 aastaks;

[RT I, 27.08.2022, 1- jõust. 01.01.2023]

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 ning Majandus- ja Kommunikatsiooniministeriumi koostatud küberturvalisuse riskianalüüsid, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel kuni 20 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

32¹⁾ seire-, järelevalvetoimingute ja küberintsidentide analüüsi käigus kogutud teave põhiseadusliku institutsiooni, valitsusasutuse, selle hallatava riigiasutuse, elutähtsa teenuse osutaja ning Eestis paikneva ja Eesti poolt tagatava julgeolekuga rahvusvahelise organisatsiooni võrgu- ja infosüsteemi, mis ei ole salastatud teabe töötlussüsteem, turvanõrkuste ja rakendatavate turvameetmete kohta, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel kuni võrgu- ja infosüsteemi kasutamise lõppemiseni, kuid mitte kauemaks kui 30 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

33) välispiiride valvamiseks mõeldud seire- ja valvesüsteemide juhtimissüsteemi ülesehitust kajastav teave kogumis. See teave salastatakse piiratud tasemel 20 aastaks;

[RT I, 27.08.2022, 1- jõust. 01.01.2023]

34) riigi infosüsteemi kuuluv asutusandmekogus Kaitseväe, jälitusasutuse, julgeolekuasutuse või tunnistajakaitset teostava asutuse poolt salajasele koostööle kaasatud isikuga, salajase koosseisulise julgeolekuasutuse ametniku või töötajaga, variisikuga, politseiagendiga, tunnistajakaitse kohaldamisega seotud isikuga või teeseldud juriidilise isiku, tema struktuuriüksuse, organi või äriühingu filiaaliga seotud füüsilise isikuga seotud variantide ja konspiratsioonivõtete rakendamist käsitlev teave, välja arvatud teave, mille avalikustamine ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel kuni 50 aastaks.

[RT I, 31.12.2021, 18- jõust. 03.01.2022]

(1¹⁾ Riigikaitseaduse tähenduses riigikaitseobjektide, välja arvatud käesoleva paragrahvi lõikes 1 nimetatud asutuste valduses olevate riigikaitseobjektide ja avaliku korra tagamiseks oluliste riigikaitseobjektide valve- ja häiresüsteemi ning kaitsemeetmeid käsitleva teabe osas on riigisadaluseks:

1) avaliku võimu organi kasutuses oleva või elutähtsa teenuse osutamisega või sisejulgeoleku tagamisega seotud riigikaitseobjekti riskianalüüs 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) Riigisadaluse ja salastatud välisteabe töötlussüsteemi käsitleva teabe osas on riigisadaluseks:

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) kiirgusturbe tagamise nõuded ja meetmed, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 30 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

3) töötlussüsteemi seadmete ja asukoha paljastava kiirguse mõõtmise meetodika ning mõõtmise tulemuste hindamise kriteeriumid. See teave salastatakse konfidentsiaalsel tasemel 25 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

3¹) 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) töötlevale üksusele spetsiaalselt salastatud teabe töötlemiseks loodud tarkvara lähtekood, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse piiratud tasemel 30 aastaks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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;

2¹) 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 töötlussüsteemiga ühendamise kohta;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

4¹) teave töötlussüsteemis rakendatavate turvameetmete kohta;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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 rajatise 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 lahingumoonaladusi käsitleva teabe osas on riigisaladuseks:

1) teave relva-, laskemoona- ja lahingumoonalao turvalisuse tagamise erinõuete kohta, välja arvatud valvesüsteemide kohta kehtestatud nõuded. See teave salastatakse piiratud tasemel 10 aastaks või kuni relva-, laskemoona- või lahingumoonalao valduse lõppemiseni;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2) Kaitseväe ja Kaitseliidu relvade, laskemoona ja lahingumoonaladude andmed kogumis. See teave salastatakse piiratud tasemel 30 aastaks.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(6) Töötleva üksuse salastatud teabekandjate evakueerimist käsitleva teabe osas on riigisaladuseks konfidentsiaalsel või kõrgemal tasemel salastatud teavet sisaldavate teabekandjate evakueerimist käsitlev § 33 lõigetes 2 ja 3 sätestatud teave. See teave salastatakse konfidentsiaalsel tasemel 20 aastaks.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(7) Töötleva üksuse turvaala valve- ja häiresüsteeme käsitleva teabe osas on riigisaladuseks:

1) teave, mis sisaldab andmeid 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) 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) 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, 31.05.2023, 3- jõust. 05.06.2023]

(7¹) Kui töötleva üksuse turvaala elektrooniline läbipääsu- või valvesüsteem on suurema süsteemi osa, salastatakse vaid turvaalale paigaldatud seadmeid kajastav teave.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 katkematuks 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 valitsemisalal, 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 töötlevale üksusele 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.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 töötlevaid üksusi, kellele seda riigisaladust sisaldav teabekandja on edastatud.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 ministriumini valitsemisalasse, esitab ta taotluse Vabariigi Valitsusele Siseministeriumi 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 töötlevale üksusele on see teave edastatud. Taotlusele lisatakse selle kohta esitatud vastuväited.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 töölevaid üksusi, kellele seda riigisaladust sisaldav teabekandja on edastatud.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 töötlevatele üksustele on see teave edastatud. Taotlusele lisatakse selle kohta esitatud vastuväited.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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 ministereium sellest kõiki töötlevaid üksusi, kellele seda riigisaladust sisaldav teabekandja on edastatud.

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

(4) Töötlev üksus, kes on edastanud teise töötleva üksuse koostatud salastatud teabekandja, mille salastamisandmed on parandatud, „Riigisaladuse ja salastatud välisteabe seaduse“ § 35 lõikes 3 nimetatud töötlevale üksusele, teavitab salastamisandmete muutmisest viivitamata seda töötlevat üksust.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

4. peatükk

SALASTATUD TEABE KAITSE KORRALDAMISE NÕUDED

§ 22. Töötleva üksuse salastatud teabe kaitse juhendile esitatavad nõuded

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Töötleva üksuse salastatud teabe kaitse juhendis reguleeritakse järgmisi küsimusi, arvestades töötleva üksuse eripära:

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 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 juurdepääsustifikaadi 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 töötlevas üksuses kehtivate selliste kordade, juhendite ja muude eeskirjade kohta, mis reguleerivad riigisaladuse töötlemist;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 12) salastatud teabekandja hävitamise meetod ja kord;
- 13) administratiivala ulatus;
- 14) relva ning tehnilise vahendi ja muu eseme, mida saab kasutada tehnilise vahendina teabe kogumiseks, turvaalale viimise kord;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 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;

17) selle riigisaladuseks oleva teabe salastatuse taseme määramise kord, mida võib käesoleva määruse kohaselt salastada mitmel tasemel.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2) Lisaks lõikes 1 nimetatutele võib salastatud teabe kaitse juhendis sätestada näiteks:

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 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) küllalise turvaalale lubamise erisused võrreldes samas töötlevas üksuses töötavate isikutega.

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

- 7) [kethetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 23. Töötleva üksuse riigisaladuse kaitset korraldava isiku või struktuuriüksuse ja infoturbejuhi tegevusele esitatavad nõuded

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

(1) Töötleva üksuse riigisaladuse kaitset korraldav isik või struktuuriüksus peab:

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 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) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 6) pidama arvestust töötajate riigisaladusele juurdepääsu lubade ja juurdepääsustifikatsioonide üle ning tagama, et riigi julgeoleku volitatud esindajal on ajakohane info „Riigisaladuse ja salastatud välisteabe seaduse“ § 20 lõike 5 alusel määratud ametikohtade kohta;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 7) pidama arvestust salastatud teabekandjate üle ning kontrollima nende olemasolu ja terviklikkust vastavalt §-le 23¹;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 8) pidama seifide kasutajate nimekirja;
- 9) edastama iga 90 päeva järel vastavalt Kaitsepolitseiametile, Kaitsevägele 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 teenistusväliste 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;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 11) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 12) osalema süsteemi turbejuhendi ja kasutusjuhendi väljatöötamises ning tagama nende tutvustamise ja kättesaadavuse;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 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) tagama teabele juurdepääsu andvate füüsiliste ja elektrooniliste vahendite väljastamise ning selliste vahendite perioodilise vahetamise ja nende üle arvestuse pidamise;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 15) omama ülevaadet töötlussüsteemide hooldamise ja remontimise ning nende konfiguratsiooni muutmise dokumentatsioonist;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 16) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

- 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]

- 18¹) 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]

18²⁾ 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.

(1¹⁾ Töötlussüsteemi eest vastutava töötleva üksuse infoturbejuht peab osalema töötlussüsteemi:

- 1) turvariskide hindamisel;
- 2) oluliste muudatuste planeerimises;
- 3) turbejuhendi ja kasutusjuhendi väljatöötamises.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

(2) Töötleva üksuse riigisaladuse kaitset korraldaval isikul või struktuuriüksuse asjaomastel töötajatel või ametnikel peab olema töötleva üksuse töödeldava teabe kõrgeimale salastatuse tasemele vastav juurdepääsuõigus.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(3) Töötlussüsteemi eest vastutava töötleva üksuse infoturbejuhil peab olema töötlussüsteemis töödeldava teabe kõrgeimale salastatuse tasemele vastav juurdepääsuõigus.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

§ 23¹. Teabekandjate kontrollimine

(1) Töötlev üksus kontrollib tema valduses olevaid salajasel ja täiesti salajasel tasemel salastatud teavet sisaldavaid registreeritud teabekandjaid järgmiselt:

- 1) füüsilise teabekandja olemasolu ja terviklikkust kontrollitakse vähemalt kord aastas vahetult;
- 2) töötlussüsteemiga püsivalt ühendamata salvestuskandja olemasolu kontrollitakse vähemalt kord aastas vahetult;
- 3) töötlussüsteemiga püsivalt ühendatud salvestuskandja olemasolu kontrollitakse vähemalt kord aastas töötlussüsteemi tarkvara abil, sobivate vahendite puudumise korral vahetult;
- 4) faili olemasolu kontrollitakse vähemalt kord aastas töötlussüsteemi tarkvara abil või pisteliselt vahetult.

(2) Arhiivihoidlas olevate salajasel ja täiesti salajasel tasemel salastatud teavet sisaldavate registreeritud teabekandjate olemasolu ja terviklikkust kontrollitakse lõikes 1 nimetatud viisil vähemalt kord viie aasta jooksul.

(3) Teabekandjaid kontrollinud füüsiline isik vormistab kontrolli tulemused kirjalikku taasesitamist võimaldavas vormis ja esitab need töötleva üksuse riigisaladuse kaitset korraldavale isikule.

(4) Töötlussüsteemi tarkvara abil tehtud kontrolli tulemused võib salvestada logifailidena.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

5. peatükk SALASTATUD TEABE JA SALASTATUD TEABEKANDJA TÖÖTLEMISE NÕUDED

1. jagu Turvaala ja administratiivala

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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 Kaitsepolitsei ameti, Kaitseväge 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, kui võrd käesolevas määruses ei ole sätestatud teisiti.

(4¹) Turvaalale esitatavad nõuded täpsustatakse juhendis, mille töötab välja Kaitsepolitseiamet koostöös Kaitseväge ja Välisluureametiga.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

§ 25. Turvaala asukoht

(1) Töötleva üksuse turvaala peab asuma tema otseses valduses olevates ruumides.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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, Kaitseväge või Välisluureametiga. 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, 31.05.2023, 3- jõust. 05.06.2023]

(2¹) 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 kasutuselevõtmisel teavitab julgeolekuasutus teist julgeolekuasutust kirjalikult esimesel võimalusel.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2²) Kaitsevägi võib võtta lisaõppekogunemise korraldamise otsuse järel lisaõppekogunemise ajaks liikuva või ajutise turvaala kasutusele Kaitseväge juhataja või tema volitatud ülema otsusel, teavitades sellest kirjalikult esimesel võimalusel Kaitseväes riigisaladuse kaitset korraldavat struktuuriüksust.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

(3¹) Liikuva või ajutise turvaala, millel töödeldakse salastatud välisteavet, kasutusele võtmise korral teavitab lõikes 2 nimetatud juhul kooskõlastuse andnud asutus ning lõigetes 2¹ ja 2² nimetatud juhul turvaala kasutusele võtnud asutus riigi julgeoleku volitatud esindajat kirjalikult esimesel võimalusel.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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) Liikuvale ja ajutisele turvaalale 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 liikuvale või ajutisele turvaalale 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 ümbritsevasse ruumidesse.

§ 28. Turvaala uks

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

(2) Turvaala ukse hingedepoolisel küljel peavad olema turvatapid, mis ukse sulgemisel sulguvad lengi sisse. Turvaala uksele peab olema automaatne sulgur, mis tagab ukse iseenesliku sulgemise määratud aja jooksul, ja andur, mis annab märku, 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 ukسلukud ei tohi olla avatavad sama võtmega, millega saab avada hoones asuvaid teisi mehaanilisi ukسلukke. Kui seda nõuet ei ole võimalik järgida, tuleb võtmeid hoida samadel tingimustel seifivõtmega.

§ 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 vältida turvaalale tehniliste seadmete ebaseaduslik paigaldamine või turvaalal hoitava salastatud teabekandjal sisalduva teabe muul viisil ohustamine.

§ 31. Avatud hoiuala

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

§ 32. Liikuv ja ajutise turvaala konstruktsiooniline kaitse

(1) Liikuv 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) Liikuv 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 määratud iga ohuolukorra kohta tuleb ette näha, kuidas toimub evakuatsioon või hävitamine, kes seda korraldavad, milliseid vahendeid selleks kasutatakse, kuhu evakueeritakse salastatud teabekandjad.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2. jaotis Turvaala valve nõuded

§ 34. Turvaala valve üldnõuded

(1) Turvaala valvamiseks peab olema valve- ja häiresüsteem (edaspidi *valveseadmestik*), läbipääsusüsteem ja mehitatud valve.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2) Turvaala valveseadmestik ja läbipääsusüsteem koos füüsilise kaitse meetmetega peavad tagama, et mehitatud valve jõuab reageerida sissetungikatsesele enne, kui sissetungija on ületanud füüsilised tõkked.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

§ 35. Valveseadmestiku nõuded

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Valveseadmestik peab:

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

1) andma häire kohe mehitatud valvele ja töötleva üksuse juhi määratud isikule, kui toimub sissetung või selle katse või kui on tekkinud valveseadmestiku rike;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2) [kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

3) võimaldama turvaala valvet eraldi sisse ja välja lülitada;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

4) automaatselt tuvastama valveseadmestiku rikked;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

5) võimaldama koostoimes läbipääsusüsteemiga kindlaks teha isiku turvaalale ning võimaluse korral ka turvaala osasse sisenemise ja sealt väljumise;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

6) võimaldama elektrooniliselt tuvastada turvaala valve sisse- ja väljalülitamise, häire aja ning koostoimes läbipääsusüsteemiga isiku turvaalale ning võimaluse korral selle osasse sisenemise ja sealt väljumise. Nimetatud toiminguid andmeid säilitatakse vähemalt üks aasta.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2) [Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(4) Valveseadmestiku keskseade ja selle juhtseade peavad asuma turvaalal. Administratiivalal võib asuda vaid selline juhtseade, mis võimaldab turvaala valvet juhtida või seadistada üksnes valveseadmestiku eriõigustega kasutajal või turvaala valvet üksnes sisse ja välja lülitada.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 36. Liikuva ja ajutise turvaala mehitatud valve

(1) Liikuvat või ajutist turvaala peavad kaitsma liikuvad või püsipositsioonidel relvastatud valvurid, kes jälgivad kogu kaitstavat ala. Turvaala valvamiseks võib kasutada nii valvemeeskonna valvureid kui ka turvaalal ööpäevaringselt töötavaid instrueeritud isikuid.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2) Kui liikuva või ajutise turvaala pidevat mehitatust ei suudeta tagada, siis tuleb liikuvale või ajutisele turvaalale paigaldada häiresüsteem, mis edastab häire valvemeeskonnale või instrueeritud turvaala töötajatele, kes peavad jõudma turvaalale kooskõlastava asutusega kooskõlastatud reageerimisaja jooksul. Reageerimisaeg ei tohi olla pikem ajast, mis kulub sissetungijal füüsiliste tõkete ületamiseks.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 37. Kohapealse mehitatud valve ringkäigud

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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, teadmismisvajadust 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 salastatud teabe kaitse juhendis sätestatud korras.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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:

- 1) kui turvaala koosneb ühest või kahest ruumist;
 - 2) riiklikult olulise välisvisiidi või kõrgete külaliste Eesti visiidi delegatsiooni liikmele.
- [RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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. Riiklikult olulise välisvisiidi või kõrgete külaliste Eesti visiidi delegatsiooni liikme võib identifitseerida muul viisil.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 teadmismajaduse põhimõtet.

§ 42. Liikval ja ajutisel turvaalal töötamise nõuded [RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 ja tehnilise vahendi abil osalejad peavad tagama, et koosolekule on juurdepääs ainult isikutele, kellele on käsitletava taseme salastatud teabele juurdepääsu õigus ning teadmismajadus;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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 kontrollimine [RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Perioodiliselt tuleb kontrollida, et koosolekuruumis ei oleks ebaseaduslikult teabe kogumise seadmeid.

(2) Koosolekuruumis ei tohi koosoleku pidamise ajal olla ühtegi eelnevalt kontrollimata eset ega tehnilist vahendit, mida saab kasutada teabe ebaseaduslikuks kogumiseks.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 46. Koosoleku salvestamine ja koosolekul märkmete tegemine [RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Koosoleku salvestamine ja koosolekul märkmete tegemine on lubatud üksnes koosoleku korraldaja nõusolekul.

(2) Iga koosolekul osaleja koosolekul tehtud salvestusi ja märkmeid sisaldavaid teabekandjaid töödeldakse vastavalt nendes sisalduva teabe salastatuse tasemele.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

5. jaotis

Administratiivala üldnõuded

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 46¹. Administratiivala üldnõuded

(1) Administratiivalal peab olema selgelt määratletud välispiir, millel on võimalik kontrollida kõiki sisse- ja väljapääse, ning sisse- ja väljapääsukontrolli süsteem, mis võimaldab tuvastada kõik sisenenud isikud ja sõidukid.

(2) Administratiivalale esitatavad nõuded täpsustatakse juhendis, mille töötab välja Kaitsepolitseiamet koostöös Kaitseväge ja Välisluureametiga.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

6. jaotis

Salastatud teabe töötlemine turvaalal ja administratiivalal

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 46². Salastatud teabe töötlemine turvaalal ja administratiivalal

(1) Töötlev üksus töötleb oma valduses olevat salastatud teavet üldjuhul oma turvaalal.

(2) Salastatud teabe töötlemine teise töötleva üksuse turvaalal on lubatud üksnes Kaitsepolitsei ameti, Kaitseväge või Välisluure ameti nõusolekul. Nimetatud nõusoleku andmisel piirdatakse nende turvaala nõuete hindamisega, mille täitmise tuvastamine oli turvaalal salastatud teabe töötlemise lubatavaks pidamise eelduseks.

(3) Ilma lõikes 2 sätestatud kooskõlastava asutuse nõusolekuta võib salastatud teavet töödelda:

- 1) selle töötleva üksuse turvaalal, kelle ametnikul või töötajal on konkreetse töödeldava teabe suhtes teadmismajadus, tingimusel, et see ametnik või töötaja viibib vahetult teabe töötlemise juures;
- 2) julgeolekuasutuse turvaalal;
- 3) välisesinduse turvaalal;
- 4) Kaitsemisteeriumi ja selle valitsemisala valitsusasutuse turvaalal.

(4) Töötlev üksus võib piiratud tasemel salastatud teavet töödelda ka oma valduses oleval administratiivalal või teise töötleva üksuse nõusolekul ka tema administratiivalal.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2. jagu

Salastatud teabe arvestus

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 46³. Salastatud teabe kogumi salastatuse tase

Kui salastatud teabe või teabekandjate kogum koosneb salastatuse eri tasemega osadest, loetakse teabe kogumi, seda kogumit kandva teabekandja ning teabekandjate kogumi salastatuse tasemeks nende osade kõrgeim salastatuse tase.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 47. Salastatud teabekandjate registreerimise üldnõuded

[Keehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 47¹. Salastatud teavet sisaldav salvestuskandja

Salastatud teavet sisaldava salvestuskandjana käsitatakse ja töödeldakse kuni hävitamiseni salvestuskandjat:

- 1) millele on salvestatud salastatud teavet, sõltumata sellest, kas teave on hiljem kustutatud, välja arvatud juhul, kui Kaitsepolitsei amet või Välisluure amet on intsidendi käsitlemise ajal määranud teisiti;
- 2) mis on töötlussüsteemi osa, sõltumata sellest, kas salvestuskandja on töötlussüsteemi tehnilise lahenduse järgi ette nähtud salastatud teabe salvestamiseks, välja arvatud juhul, kui Välisluure amet on töötlussüsteemi akrediteerimisel määranud teisiti.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 48. Teabekandja originaal

(1) Teabekandja originaaliks loetakse töötleva üksuse loodud teabekandja esimest registreeritud eksemplari. Teabekandja muid eksemplare ning teisest töötlevast üksusest saabunud teabekandjaid käsitatakse ja töödeldakse koopiadena.

(2) Töötleva üksuse valduses oleva füüsilise teabekandja originaali edastamise korral teisele töötlevale üksusele tehakse sellele lisamärke „Originaal“. Sellise märkega teabekandjat käsitatakse originaalina ja töödeldakse vastavalt.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 49. Salastatud teabekandjate register

(1) Töötlev üksus peab salastatud teabekandjate registreerimiseks sisse seadma salastatud teabekandjate registri (edaspidi ka *register*).

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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) Register võib jaguneda põhiregistriks ning allregistriteks. Allregistri sisseseadmise otsustab töötleva üksuse juht.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 50. Nõuded registrile

(1) Registrit peetakse elektrooniliselt või vajaduse korral paberil.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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) Teabekandja kohta märgitakse registrisse järgmine teave selle olemasolu korral:

1) teabekandja identifitseerimiseks vajalikud andmed: registreerimiskuupäev ja -number, selle loonud töötleva üksuse nimi ning dokumendi puhul ka pealkiri ning dokumendi koostanud ja allkirjastanud või sisu kinnitanud isiku nimi. Koopiale ei pea andma uut registreerimisnumbrit, kui märgitakse koopia järjekorranumber;

2) teabekandja edastanud töötleva üksuse nimi, registreerimiskuupäev ja -number, kui teabekandja on saabunud teisest töötlevast üksusest;

3) teabekandja liik;

4) teabekandja salastamisalus, salastatuse tase ja salastamistähtaeg, nende muudatus ja muudatuse tegemise alus;

5) füüsilise teabekandja puhul selle eksemplaride arv ja numbrid. Eksemplaride arvu ja numbreid ei pea registrisse kandma konfidentsiaalsel ja madalamal tasemel salastatud teabekandja puhul;

6) füüsilise teabekandja puhul selle osade ja dokumendi lehtede arv. Kui dokument on vormistatud lehe mõlemale poolele, registreeritakse registris selle dokumendi lehtede arv, märkides juurde, et dokument on vormistatud lehe mõlemale poolele;

7) füüsilise teabekandja puhul koopiate arv. Koopiate arvu ei pea registrisse kandma konfidentsiaalsel ja madalamal tasemel salastatud teabekandja puhul;

8) selle töötleva üksuse nimi, kellele teabekandja edastati, ja edastamise aeg, füüsilise teabekandja puhul üleandmis-vastuvõtmisakti number;

9) märgete kohta, kui teisele töötlevale üksusele on antud nõusolek edastada teabekandjal sisalduvat salastatud teavet kolmandale töötlevale üksusele;

10) märgete kohta, sealhulgas hävitamise akti registreerimiskuupäev ja -number;

11) selle isiku nimi, kellele on antud juurdepääs salajasel või kõrgemal tasemel salastatud teabekandjal olevale teabele, ning juurdepääsu andmise viis ja aeg;

12) teabekandjale määratud lisaturvameetmed, kui need rakenduvad registrit pidavale töötlevale üksusele, ja teabekandja suhtes teadmismisvajadust omava selle isiku nimi või ametikoht, kes on seotud registrit pidava töötleva üksusega;

13) elektroonilise dokumendi puhul teave, mis võimaldab kontrollida dokumendi terviklikkust.

(2) Salvestuskandja kohta märgitakse registrisse järgmine teave selle olemasolu korral:

1) salvestuskandja identifitseerimiseks vajalikud andmed: registreerimiskuupäev ja -number, salvestuskandja unikaalsed tuvastamist võimaldavad andmed;

2) salvestuskandja edastanud töötleva üksuse nimi, registreerimiskuupäev ja -number juhul, kui salvestuskandja on saabunud teisest töötlevast üksusest;

3) salvestuskandja liik;

4) salvestuskandjal sisalduva teabe kõrgeim salastatuse tase;

5) selle töötleva üksuse nimi, kellele salvestuskandja edastati, ning edastamise aeg ja üleandmis-vastuvõtmisakti number;

6) märgete kohta, kui teisele töötlevale üksusele on antud luba edastada salvestuskandjal sisalduvat salastatud teavet kolmandale töötlevale üksusele;

7) märgete kohta, sealhulgas hävitamise akti registreerimiskuupäev ja -number;

8) selle isiku nimi, kellele salajasel või kõrgemal tasemel salastatud salvestuskandja üle anti, ja üleandmise aeg;

9) salvestuskandjale määratud lisaturvameetmed, kui need rakenduvad registrit pidavale töötlevale üksusele, ja salvestuskandja suhtes teadmismisvajadust omava selle isiku nimi või ametikoht, kes on seotud registrit pidava töötleva üksusega.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 52. Salastatud teabekandjate registreerimine

(1) Salastatud teabekandja registreeritakse hiljemalt selle valmimisele või saabumisele järgneval tööpäeval. Salastatud teabekandja loetakse valminuks üldjuhul selle allkirjastamisel või elektroonilisel kinnitamisel. Salvestuskandja registreeritakse hiljemalt selle kasutusele võtmisel.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 registreerimiseks sisse seatud registris.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(5) Registreerima ei pea:

1) töötlussüsteemis töödeldavat elektroonilist sõnumit, kui teabe töötlemine on töötlussüsteemi tarkvara abil fikseeritud;

2) töötlussüsteemis töödeldavat salajasel või kõrgemal tasemel salastatud teabekandjast tehtud koopiat, kui teabe töötlemine on töötlussüsteemi tarkvara abil fikseeritud.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 53. Registripidaja ja registrikande tegija

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Registri ja sellesse kantud teabe haldamist korraldaval isikul (edaspidi *registripidaja*) peab olema registreeritavate teabekandjate kõrgeimale salastatuse tasemele juurdepääsu õigus.

(2) Registripidajad ja muud registrikannete tegemise õigusega isikud ning nende isikute õiguste ulatuse määrab töötleva üksuse juht või tema volitatud isik.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 53¹. Salastatud teabekandja üleandmine töötleva üksuse siseselt

(1) Füüsilise teabekandja teisele sama töötleva üksusega teenistus- või lepingulises suhtes olevale füüsilisele isikule üleandmine tuleb fikseerida kirjalikult teabekandjast eraldi või elektroonilise kinnitusega dokumendihaldussüsteemis.

(2) Üleandmise kohta märgitakse:

1) teabekandja registreerimiskuupäev ja -number, kõrgeim salastatuse tase ning üleantavate ühikute arv;

2) üleandmise kuupäev ja kellaaeg;

3) vastuvõtja nimi ja allkiri või elektrooniline kinnitus;

4) üleandja nimi ja allkiri või elektrooniline kinnitus.

(3) Andmeid salastatud teabekandja üleandmise kohta säilitatakse turvaalal või dokumendihaldussüsteemis vähemalt kümme aastat. Füüsilise teabekandja, millel on fikseeritud andmed salastatud teabekandja üleandmise kohta, võib hävitada pärast viie aasta möödumist, kui see on digiteeritud.

(4) Käesolevat paragrahvi ei pea kohaldama konfidentsiaalsel tasemel salastatud teabekandja registreerimata koopia ja piiratud tasemel salastatud teabekandja üleandmisel.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 54. Salastatud teabega tutvumise kinnitus

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Salajasel ja kõrgemal tasemel salastatud teabekandjas sisalduva teabega tutvumise kohta annab isik allkirja tutvumislehele või elektroonilise kinnituse.

(2) Töötlussüsteemis ei ole eraldi tutvumise kinnitus vajalik, kui elektrooniliselt tagatakse tutvuja isiku ja tutvumisaja tuvastatavus.

(3) Kui allkirja või elektroonilise kinnituse andmine ei ole teabekandjas sisalduva teabega tutvumise ajal võimalik, fikseeritakse tutvuja isik ja tutvumisaeg muul viisil ning võetakse allkiri või kinnitus esimesel võimalusel. Kui tutvuja on välisriigi kodanik ning tema isik ja tutvumisaeg on fikseeritud muul viisil, ei pea allkirja või kinnitust võtma.

(4) Tutvumislehti ja muid andmeid teabega tutvumise kohta säilitatakse vähemalt 75 aastat, kuid mitte vähem, kui säilitatakse teabekandjat, milles sisalduva teabega tutvuti.

(5) Füüsilisel teabekandjal oleva tutvumislehe võib hävitada pärast viie aasta möödumist, kui see on digiteeritud.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

3. jagu

Salastatud teabe märgistamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

1. jaotis

Märgistamise üldnõuded

§ 54¹. Salastatud teabe, teabekandja ja teabekandjate kogumi märgistamise üldpõhimõtted

(1) Salastatud teave ja teabekandja märgistatakse selle tüüpi ja omadusi arvestades parimal võimalikul moel, mis ei kahjusta teabe ega teabekandja terviklikkust, eesmärgiga, et:

1) selle valdajal oleks võimalik üheselt aru saada, et tegemist on salastatud teabega;

2) selle mis tahes viisil töötlejal oleks võimalik saada teada selle salastatuse tase, salastamisalus, salastamistähtaeg ning registreerimiskuupäev ja -number, samuti lisaturvameetmed ja teabekandja suhtes teadmisyajadust omavad isikud, kui need on määratud.

(2) Salastatud teabekandjate kogum märgistatakse lisaks lõikes 1 sätestatule viisil, mis võimaldab üheselt aru saada, et tegemist on teabekandjate kogumiga.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 55. Riigisaladust sisaldava salastatud teabekandja märgistamine

(1) Riigisaladust sisaldavale salastatud teabekandjale tehakse järgmine märgistus:

- 1) salastatuse taseme märke;
- 2) salastamisaluse märke;
- 3) salastamistähtaja märke.

(2) Salastatuse taseme märkeks on teabekandja kõrgeimale salastatuse tasemele vastav tekst „täiesti salajane“, „salajane“, „konfidentsiaalne“ või „piiratud“. Salastatuse taseme märke tehakse trükituna sõrendatud paksus kirjas vähemalt 16-punktiste suurtähtedega või samadele nõuetele vastavat punast värvi teksti kandva templijäljendi või kleepsuga.

(3) Salastamisaluse märkeks on tekst „Riigisaladus ... alusel“, mille lünka kantakse viide käesolevale määrusele ning selle asjaomasele paragrahvile, lõikele ja punktile. Kui salastatud teabekandja on salastatud mitmel õiguslikul alusel, kantakse lünka kõik alused.

(4) Registreeritud teabekandjale või selle juurde kantakse lisaks lõikes 1 nimetatud märgistusele registreerimiskuupäev ja -number.

(5) Kui lõigetes 2–4 sätestatud nõuetele vastavat märgistust ei ole võimalik teabekandja tüübi, materjali, suuruse või muu omaduse tõttu teabekandjale teha, võib rakendada ühte või mitut järgmistest eranditest, tingimusel et märgistus on hõlpsasti nähtav ja loetav ning § 54¹ lõikes 1 nimetatud eesmärk on täidetud:

- 1) teha märgistuse muul viisil või tihedamas, õhemas, väiksemas, väiketähtedega või teist värvi kirjas;
- 2) teha ainult salastatuse taseme märkest ning registreerimiskuupäevast ja -numbrist koosneva märgistuse;
- 3) teha märgistuse teabekandja asemel selle ümbrisele, pakendile või teabekandja külge kinnitatud sildile.

(6) Kui lõigetes 2–4 sätestatud nõuetele vastava märgistuse tegemine ohustab teabekandjale kantud riigisaladuse salastatust, võib jätta teabekandja märgistamata tingimusel, et § 54¹ lõikes 1 nimetatud eesmärk on muul viisil täidetud.

(7) Riigisaladust sisaldava teabekandja edastamisel välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile tehakse teabekandjale välislepingu nõuetele vastav salastatuse taseme märke ning esilehele inglise keeles märke „Classified as State Secret of the Republic of Estonia“.

(8) Salastatud teabekandja nõuetekohase märgistamise eest vastutab teabekandja koostaja.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 56. Salastatud välisteavet sisaldava teabekandja märgistamine

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 57. Salastatud teabekandja koopia ja väljavõtte märgistamine

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 58. Lisamärgistus turvameetmete ja teadmismajadusega isikute kohta

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

Salastatud teabekandjale võib märgistuse juurde või muule selgelt nähtavale kohale teha lisamärke lisaturvameetmete või teabekandja suhtes teadmismajadust omava isiku nime või ametikoha kohta.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 59. Pakendatud teabekandja ja teabekandjate kogumi lisamärgistamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Kui säilitamiseks pakendatud salastatud teabekandjat säilitatakse pakendis, ümbrises või muul viisil nii, et märgistus on varjatud, tehakse pakendile või ümbrisele hõlpsasti nähtav ja selgelt loetav lisamärgistus.

(2) Vedamiseks pakendatud salastatud teabekandja märgistamisele kohaldatakse § 88.

(3) Kui salastatud teabekandjad moodustavad kogumi, tehakse kogumi ümbrisele hõlpsasti nähtav ja selgelt loetav ning kogumi kõrgeimale salastatuse tasemele vastav lisamärgistus.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 60. Märgistuse muutmine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Salastatuse kustumise korral tehakse lisamärgistus või muudetakse märgistust viisil, mis võimaldab valdajal aru saada, et enam ei ole tegemist salastatud teabekandjaga.

(2) Kui teabekandja võimaldab, märgitakse salastatuse ennetähtaegsel kustutamisel teabekandjale või selle juurde tekst „Salastatus kustutatud ... alusel“, mille lünka kantakse kustutamise otsuse teinud organi nimi ning otsuse rekvisiidid ja jõustumise aeg.

(3) Kui teabekandja võimaldab, märgitakse salastamistähtaaja pikendamisel teabekandjale või selle juurde tekst „Salastamistähtaeg pikendatud ... alusel“, mille lünka kantakse pikendamise otsuse teinud organi nimi ja otsuse rekvisiidid, ning märgitakse uus salastamistähtaeg.

(4) Kui teabekandja võimaldab, tehakse salastamisandmete parandamisel lisamärgistus või muudetakse valet märgistust ja märgitakse teabekandjale või selle juurde tekst „Salastatus parandatud ...“, mille lünka kantakse salastamisandmete parandamise otsuse teinud organi või ametniku nimi ja ametniku allkiri ning otsuse rekvisiidid.

(5) Teabekandja märgistust muudetakse ja selle kohta tehakse kanne registrisse esimesel võimalusel.

(6) Arhiivihoidlas oleva teabekandja märgistust muudetakse selle töötlemise korral, välja arvatud vahetult selle hoidmisega ja säilitamisega seotud toimingute korral.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2. jaotis

Dokumendi märgistamine

§ 61. Dokumentide vormistamise üldnõuete kohaldamine

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 62. Lehekülgede nummerdamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Paberdokumendi iga leht nummerdatakse ja igale lehele märgitakse lehtede koguarv. Kui dokument on vormistatud lehe mõlemale poolele, tuleb nummerdada ja märkida vastavalt leheküljed.

(2) Elektroonilise dokumendi iga lehekülg nummerdatakse alates esimesest ja igale leheküljele märgitakse lehekülgede koguarv.

(3) Kui paberdokument ei võimalda lehekülgi nummerdada, peavad selle juures olema muud teabe teraviklikkuse kontrollimist võimaldavad andmed. Kui elektrooniline dokument või selle teabekandja ei võimalda

lehekülgi nummerdada, peavad võimaluse korral selle juures olema muud teabe terviklikkuse kontrollimist võimaldavad andmed.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 63. Dokumendi märgistamine

Kui paberdokument või elektrooniline dokument ja selle teabekandja võimaldavad, märgistatakse salastatud dokument järgmiselt:

1) riigisaladust sisaldaval dokumendil tehakse salastamisaluse ja salastamistähtaja märges esilehe päise paremasse nurka, registreerimiskuupäev ja -number selgelt nähtavale kohale ning salastatuse taseme märges iga lehekülje päise ja jaluse keskele;

2) salastatud välisteavet sisaldaval dokumendil tehakse § 118¹ lõikes 1 sätestatud märgistus esimesele leheküljele ning sama paragrahvi lõikes 3 sätestatud lisamärges esilehe päise paremasse nurka.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 64. Dokumendi lisa, koopia ja väljavõtte märgistamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Dokumendi lisa, mis on kasutatav põhidokumendita, märgistatakse nagu eraldi dokument.

(2) Paberdokumendi koopia tehakse lisamärges „Koopia“.

(3) Dokumendi väljavõtte tehakse lisamärges „Väljavõte“ ja viide originaaldokumendile.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 65. Tekstiosade ja illustratsioonide kaupa märgistamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Kui dokumendi tekstiosadel või illustratsioonidel on erinev juurdepääsupiirangu tase või erinevad salastatud välisteabe avaldajad, võib dokumendi märgistada tekstiosade või illustratsioonide kaupa.

(2) Lõikes 1 nimetatud märgistus tehakse sulgudes suurtähtedega asjaomase lõigu algusesse või illustratsiooni ette või peale ning vajaduse korral ka lõigu lõppu või illustratsiooni järele või alla.

(3) Tekstiosa või illustratsiooni juurdepääsupiirangu taseme märges võib esitada sulgudes lühendina, kasutades riigisaladuse puhul märkeid „P“, „K“, „S“ või „TS“.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 67. Dokumentide kogumi märgistamine

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

(2) Toimikuks liidetud või muul viisil kaante vahele kogutud paberdokumentide kogumi kõrgeima salastatuse taseme märges tehakse selle esi- ja tagakaane päisesse ja jalusesse.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(3) Muudel juhtudel tehakse kogumi kõrgeima salastatuse taseme märges selle esimeseks dokumendiks oleva dokumendi esimese lehekülje päisesse ja jalusesse.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(4) Kui kogumi esimene lehekülg ei sisalda riigisaladust, tehakse dokumendi päise paremasse nurka lisamärges „Märgistatud riigisaladusena kui kogumi esileht“.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

3. jaotis Muu teabekandja märgistamine

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 68. Salastatud foto, transporendi ja slaidi märgistamine

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 69. Heli-, filmi- ja videosalvestise märgistamine

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

4. jaotis

Faili ja elektroonilise sõnumi märgistamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 70. Faili märgistamine

Kui fail seda võimaldab, märgitakse salastatud teavet sisaldava faili salastatuse tase suurtähtedega faili nime algusesse ning failide kogumi kõrgeim salastatuse tase kogumi nime algusesse. Kui faili või failide kogumi nime alguses on kuupäevamärge, võib salastatuse taseme märkida pärast kuupäevamärget. Märke võib vajaduse korral esitada sulgudes või visuaalselt muul viisil eristuvalt lühendina, kasutades riigisaladuse puhul märkeid „P“, „K“, „S“ või „TS“.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 71. Elektroonilise sõnumi märgistamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

Elektroonilise sõnumi salastatuse taseme märke tehakse suurtähtedega sõnumi sisuosa algusesse ning vajaduse korral ka sõnumi pealkirja või teemarea algusesse ja sõnumi sisuosa lõppu. Sõnumi pealkirja või teemarea algusesse tehtava märke võib vajaduse korral esitada sulgudes või visuaalselt muul viisil eristuvalt lühendina, kasutades riigisaladuse puhul märkeid „P“, „K“, „S“ või „TS“.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

4. jagu Salastatud teabekandja säilitamine

1. jaotis Säilitamistingimustele ja -vahenditele esitatavad nõuded

§ 72. Seif

(1) Konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandjaid säilitatakse murdmiskindlas koodlukuga seifis. Seifi kasutuselevõtmine tuleb eelnevalt kooskõlastada vastavalt Kaitsepolitsei ameti, Kaitseväge või Välisluureametiga, välja arvatud juhul, kui seifi murdmiskindlus vastab vähemalt standardi EVS-EN 1143-1 1. klassi nõuetele.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 teadmisyajaduse põhimõttest. Seifil peavad niisugusel juhul olema eraldi lukustatavad osad.

(5) Kooskõlastava asutuse loal võib salastatud teabekandjaid säilitada avatud hoiualal. Luba andes võib määrata avatud hoiualal säilitamise lisatingimusi, sealhulgas teabe kõrgeima salastatuse taseme, säilitamise viisi ja lisakaitsemeetmed.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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 lehekülj 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 liikuvale ja ajutisele turvaalale kasutada § 72 lõikes 1 sätestatud 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 hankimise, säilitada metallist dokumendikapis või sahtlis, kui hoidmispaik asub turvaalal ja on varustatud vähemalt ühe sulgemisrauaga või kolmeosalise võtmekombinatsiooniga lukuga.

(5) Töötlussüsteemi osaks olevat salvestuskandjat võib säilitada olenevalt salastatuse tasemest turvaalal või administratiivalal asuva arvuti sees ilma salvestuskandjat seifi või kappi lukustamata, kui Välisluureamet on andnud töötlussüsteemi akrediteerimisel selleks nõusoleku.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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, telefoninumbriid, aritmeetilised jadad.

(3) Lukukoodi 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 võib seifi võti asuda seifi kasutaja käes.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2) Kui konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandjate hoiustamiseks kasutataval seifil on lisaks koodlukule ka võti ning seifi kasutaja lahkub turvaalalt või seda ümbritsevalt administratiivalalt avalikku ruumi, tuleb seifi võti lukustada võtmete kappi.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 varuvõtme ja lukukoodi hoidmine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Seifi varuvõti ja lukukood antakse pitseeritud ümbrikus salastatud teabe kaitse juhendis määratud isikule, kes hoiab neid eraldi seifis. Ümbrikule märgitakse lukukoodi muutmise kuupäev. Erandkorras võib kooskõlastava asutuse eelneval loal hoida varuvõtmeid ja lukukoodi muul turvalisel viisil.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

(3) Muud seifiluku koodi ülestähendused on keelatud.

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

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Piiratud tasemel salastatud teabekandja säilitamiseks kasutatava seifi, kapi või sahtli võtit või lukukoodi tuleb hoida nii, et see on kaitstud kõrvaliste isikute kätte sattumise eest.

(2) Piiratud tasemel salastatud teabekandja säilitamiseks kasutatava seifi lukukoodi muutmisel lähtutakse § 75 lõike 3 punktidest 1–3.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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) 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.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2¹) [Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

(3) Salajasel ja täiesti salajasel tasemel teabekandjat võib reprodutseerida ja sellest väljavõtte teha registripidaja või töötleva üksuse juhi või tema volitatud isiku määratud muu isik.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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.

(3) Reprodutseerimisseadmele tuleb teha selgelt loetav märgistus reprodutseerida lubatud teabe kõrgeima salastatuse taseme kohta.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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]

(1¹) Salastatud teabekandja evakuatsiooni korral võib selle hävitada väljaspool turvaala või administratiivala viisil, mis kaitseb sellel sisalduvat teavet avalikuks tuleku ning juurdepääsuõiguse ja teadmismajaduseta isiku juurdepääsu eest.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

§ 83. Salastatud teabekandja hävitamine

(1) Salajasel ja kõrgemal tasemel salastatud paberikandja hävitamiseks kasutatav paberipurustaja peab paberi purustama tükkideks, mis ei tohi olla suuremad kui 5 mm².

(2) Konfidentsiaalsel ja madalamal tasemel salastatud paberikandja hävitamiseks kasutatav paberipurustaja peab paberi purustama tükkideks, mis ei tohi olla suuremad kui 10 mm².

(3) Kui lõigetes 1 ja 2 nimetatud teabekandja purustamisel tekkinud jäätmed hävitatakse viisil, mis teeb võimatuks teabekandja taastamise, võib hävitamiseks kasutada paberipurustajat, mis purustab paberi tükkideks, mis ei tohi olla suuremad kui 30 mm².

(4) Salvestuskandja hävitamiseks kasutatav seade peab salvestuskandja purustama tükkideks, mis ei tohi olla suuremad kui:

- 1) kõvaketta puhul – 10 mm²;
- 2) optilise andmekandja puhul – 5 mm²;
- 3) pooljuhtketta puhul – 4 mm².

(5) Lõigetes 1–4 nimetatud seadmeid ja meetodeid võib salastatud teabekandja hävitamiseks kasutada vastavalt Kaitsepolitsei ameti, Kaitseväe või Välisluure ameti nõusolekul. Selleks nõusolekut andes võib määrata erandliku seadme või meetodi kasutamisele lisatingimusi, sealhulgas teabekandja liigi, sellel sisalduva teabe salastatuse taseme ja mahu ning hävitamise põhjustava ohuolukorra.

(6) Fail hävitatakse kustutamise teel.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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) Kaitsepolitsei ameti 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, välja arvatud konfidentsiaalsel tasemel salastatud teabekandja registreerimata koopia hävitamises peab osalema vähemalt kaks isikut, kes allkirjastavad salastatud teabekandja hävitamise akti või annavad elektroonilise kinnituse dokumendihaldussüsteemis.

(2) Hävitamises osalevatel isikutel peab olema asjakohasel tasemel salastatud teabele juurdepääsu õigus.

(3) Faili mustandi või faili registreerimata koopia võib hävitada isik iseseisvalt.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 86. Salastatud teabekandja hävitamise akt

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

(2) Salastatud teabekandja hävitamise aktis peavad olema märgitud:

1) teabekandja registreerimiskuupäev ja -number, eksemplari number ja hävitatavate ühikute arv ning vajaduse korral eksemplaride arv;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2) teabekandja hävitanud isikute andmed;

3) hävitamismeetod;

4) hävitamise õiguslik alus.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(3) Salastatud teabekandja hävitamise akte säilitatakse turvaalal või dokumendihaldussüsteemis vähemalt kümme aastat. Füüsilisel teabekandjal oleva hävitamise akti võib hävitada pärast viie aasta möödumist, kui see on digiteeritud.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(4) Salastatud teabekandja hävitamise akti koostamata võib hävitada:

1) konfidentsiaalsel ja madalamal tasemel salastatud teabekandja registreerimata koopia;

2) faili mustandi või faili registreerimata koopia, kui nende hävitamise toiming on töötlussüsteemisest tõendatav.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

7. jagu

Salastatud teabekandja vedamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

1. jaotis

Salastatud teabekandja vedamise üldnõuded

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 87. Vastuvõtja õigus juurde pääseda asjakohase taseme salastatud teabele

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 87¹. Salastatud teabekandja vedamise üldnõuete kohaldamine

Käesolevas jaos sätestatud nõudeid ei kohaldata avalikus ruumis töötlemiseks ette nähtud töötlussüsteemiks või selle osaks olevale kaasaskantavale töötlusseadmele ja selles olevale salvestuskandjale, mida veetakse avalikus ruumis ilma üleandmise eesmärgita.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 88. Salastatud teabekandja vedamiseks pakendamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Salastatud teabekandjat veetakse läbipaistmatus topelpakendis.

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

(3) Välispakendile märgitakse:

- 1) vastuvõtva töötleva üksuse nimi;
- 2) pakendis sisalduva teabekandja registreerimiskuupäev ja -number;
- 3) vajaduse korral vastuvõtva töötleva üksuse aadress.

(4) Sisepakendile märgitakse:

- 1) aadressaadiks vastuvõtva töötleva üksuse salastatud teabekandjate register;
- 2) pakendis sisalduva teabekandja salastatuse tase, registreerimiskuupäev ja -number ning ühikute arv;
- 3) märge „Leidmisel teavitada kohe Kaitsepolitsei ametit“.

(5) Kui teabekandjat veetakse avalikus ruumis ilma üleandmise eesmärgita, tuues selle pärast töötlemise vajaduse lõppemist tagasi töötleva üksuse administratiivalale või turvaalale, märgitakse sellise teabekandja nii välis- kui ka sisepakendile vähemalt töötleva üksuse nimi ning sisepakendile lisaks teabekandja salastatuse tase ja lõike 4 punktis 3 sätestatud märge.

(6) Piiratud tasemel salastatud teabekandja vedamiseks võib välispakendina kasutada kotti, kohvrit või muud samalaadset eset, mis on lukustatud või plommitud või suletud muul viisil, mis takistab kõrvalistel isikutel selle avamist. Sellist välispakendit ei pea märgistama.

(7) Töötlev üksus võib Kaitsepolitsei ameti nõusolekul teha käesolevas paragrahvis sätestatud salastatud teabekandja pakendamise nõuetes erandeid tingimusel, et teabekandja turvalisus tagatakse muude meetmetega.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 89. Vedamise korraldamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Enne salastatud teabekandja vedamist lepivad saatev töötlev üksus ning vastuvõttev töötlev üksus teabekandja vedamises kokku, järgides käesolevas määruses sätestatud nõudeid.

(2) Kui salastatud teabekandja vedamise kohta kehtestatud nõudeid ei ole töötleval üksusel võimalik järgida, peab ta pöörduma salastatud teabekandja vedamise korraldamiseks Kaitsepolitsei ameti või Kaitseväe poole.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 90. Vedamise viis

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Salastatud teabekandjat veetakse viisil, mis tagab, et teabekandja vedamisega seotud asjaoludest, sealhulgas selle vedamise faktist, on teadlikud üksnes isikud, kellele see on töö- või teenistusülesande tõttu vajalik.

(2) Salastatud teabekandjat veetakse viivitusega, valides vedamiseks võimalikult lühikese teekonna ja ohutu viisi.

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

(4) Kui konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandjat ei ole võimalik kohe vedada või teisele töötlevale üksusele üle anda, tagastatakse see saatva töötleva üksuse registripidajale või riigisaladuse kaitset korraldavale isikule.

(5) Piiratud tasemel salastatud teabekandjat võib teisele töötlevale üksusele saata posti teel, kui on tagatud postisaadetise teekonna jälgimine ja saadetise väljastamine allkirja vastu.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 91. Kulleri juurdepääsuõigus

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

Konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandjat vedaval kulleril peab olema asjakohasel tasemel salastatud teabele juurdepääsu õigus.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 92. Salastatud teabekandja väljaviimine turvaalalt

Konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandja võib turvaalalt välja viia üksnes saatva töötleva üksuse juhi, registripidaja või salastatud teabe kaitse juhendis määratud muu isiku loal ja vedamiseks mõeldud lukustatud kotis või kastis või plommitud diplomaatilise posti kotis.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 93. Salastatud teabekandja üleandmis-vastuvõtmisakt

(1) Salastatud teabekandja teisele töötlevale üksusele üleandmise kohta koostab saatev töötlev üksus üleandmis-vastuvõtmisakti. Piiratud tasemel salastatud teabekandja üleandmise kohta ei pea akti koostama.

(2) Üleandmis-vastuvõtmisakti märgitakse:

1) teabekandja registreerimiskuupäev ja -number, kõrgeim salastatuse tase ning üleantavate ühikute arv. Üleandmis-vastuvõtmisakti ei tohi märkida viidet teabekandjal sisalduva teabe sisu kohta;

2) vastuvõtva töötleva üksuse nimi ja aadress;

3) üleandmise kuupäev ja kellaaeg;

4) vastuvõtja ees- ja perekonnanimi ning allkiri;

5) üleandja ees- ja perekonnanimi ning allkiri.

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

(4) Üleandmis-vastuvõtmisakti säilitatakse turvaalal vähemalt kümme aastat. Füüsilisel teabekandjal oleva akti võib hävitada pärast viie aasta möödumist, kui see on digiteeritud.

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

(6) Käesolevat paragrahvi ei kohaldata teabekandjale, mida veetakse avalikus ruumis ilma üleandmise eesmärgita.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 94. Salastatud teabekandja vastuvõtja kohustused

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

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

(3) Saadetis tuleb viivitamata üle anda registripidajale, kes korraldab teabe registreerimise ja töötleva üksuse sisese edastamise salastatud teabe kaitse juhendis sätestatud korras.

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

(5) Käesolevat paragrahvi ei kohaldata teabekandjale, mida veetakse avalikus ruumis ilma üleandmise eesmärgita.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2. jaotis

Salastatud teabekandja vedamine administratiivala kaudu ühelt turvaalalt teisele

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 95. Administratiivala kaudu vedav kuller

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

Salastatud teabekandjat võib administratiivala kaudu ühelt turvaalalt teisele vedada üks kuller.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 96. Vedamise üldnõuete kohaldamine administratiivala kaudu vedamisel

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

Kui teabekandja veetakse ühelt turvaalalt teisele administratiivala kaudu, ei kohaldata §-e 88 ja 92.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

3. jaotis

Salastatud teabekandja vedamine avaliku ruumi kaudu

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 97. Avaliku ruumi kaudu vedav kuller

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Konfidentsiaalsel ja madalamal tasemel salastatud teabekandjat võib avaliku ruumi kaudu vedada üks kuller.

(2) Salajasel ja kõrgemal tasemel salastatud teabekandjat peab avaliku ruumi kaudu vedama vähemalt kaks kullerit. Kaitsepolitsei ameti, Kaitseväe, riigi julgeoleku volitatud esindaja või Välisluure ameti loal võib seda teha üks kuller.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 98. Sõiduki kasutamine avaliku ruumi kaudu vedamisel

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Salajasel ja kõrgemal tasemel salastatud teabekandjat veetakse üldjuhul autoga.

(2) Auto aknad hoitakse suletud ja ukсед lukustatud ning autojuht peab olema riigi ametiasutusega või saatva või vastuvõtva töötleva üksusega töö- või teenistussuhtes.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 99. Relva kandmine avaliku ruumi kaudu vedamisel

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Vähemalt üks täiesti salajasel tasemel salastatud teabekandjat vedav kuller peab kandma ametirelva. Kaitsepolitsei ameti, Kaitseväe, riigi julgeoleku volitatud esindaja või Välisluure ameti loal võib täiesti salajasel tasemel salastatud teabekandjat vedada ametirelva kandmata.

(2) Ainsana ametirelva kandev kuller ei või teabekandja vedamise ajal juhtida sõidukit.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

4. jaotis

Salastatud teabekandja vedamine välismaale, välismaal ja välismaalt

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 100. Välismaale, välismaal ja välismaalt kulleriga vedamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Välismaale, välismaal ja välismaalt veetakse 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 vedamiseks diplomaatilise või sõjalise kullerita juhul, kui kulleri kasutamine tooks kaasa ebasoovitava viivituse või kui teistsuguse vedamise vajadus on tingitud objektiivsest olukorrast.

(3) Kui salastatud teabekandjat soovib diplomaatilise või sõjalise kullerita vedada julgeolekuasutus, annab vedamiseks kirjaliku loa selle julgeolekuasutuse juht või tema volitatud isik.

(4) Lõikes 2 nimetatud loas esitatakse nõuded, mida peab saadetise vedamisel täitma, eelkõige teekonna ja vedamiseks kasutatavate transpordivahendite kohta.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 101. Kuller välismaale, välismaal ja välismaalt vedamisel

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

(2) Rahvusvahelise sõjalise operatsiooni piirkonnas võib salastatud teabekandjat vedada ka sõjalise kulleriga. Nõuded sõjalisele kullerile kehtestab Kaitseväge juhataja.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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) Piiratud tasemel salastatud teavet võib töödelda avalikus ruumis:

1) möödapääsmatu vajaduse korral teabe operatiivseks edastamiseks või vastuvõtmiseks, kui kasutatakse avalikus ruumis töötlemiseks ette nähtud akrediteeritud süsteemi;

2) muu vajaduse korral teabe edastamiseks või vastuvõtmiseks üksnes juhul, kui kasutatakse avalikus ruumis töötlemiseks ette nähtud akrediteeritud süsteemi osaks olevat mobiiltelefoni.

[RT I, 06.10.2021, 1- jõust. 09.10.2021]

(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.

(2¹) Kaitsevägi võib töödelda kuni salajasel tasemel salastatud operatsiooniplanimist ja operatsioonijuhtimist käsitlevat riigikaitse riigisaladust või selle sisule vastavat salastatud välisteavet avalikus ruumis, kui sellise teabe edastamine on vajalik rahvusvahelises sõjalises koostöös osalemiseks või riigi sõjaliseks kaitsmiseks ning kasutatakse avalikus ruumis töötlemiseks ette nähtud akrediteeritud süsteemi.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 juurdepääsuõiguseteta või teadmisyajaduseteta isikute juurdepääsu eest.

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

(4) Kui § 6 lõike 1 punktides 2–5 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, 06.03.2019, 7- jõust. 09.03.2019]

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 mittekesseaadavus või mittearusaadavus;
- 5) terviklikkus – teabe omadus olla volitamata isikute poolt muutmata, täiendamata või hävitamata;
- 6) oht – teabe käideldavuse, salajasuse või terviklikkuse potentsiaalne kahjustumine;
- 7) intsident – olukord, kus teave või selle kaitsmist toetavad süsteemitoimingud ja -vahendid kaotasid või võisid kaotada varguse, sabotaaži, terrorismiaktide, muu lubamatu tegevuse või turvanõrkuste tõttu salajasuse, terviklikkuse või käideldavuse (sealhulgas teabe kadumine, volitamata isikutele teatavakssaamine, volitamata isikute poolt muutmine või hävitamine või rünne süsteemi suhtes);
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 8) turvarisk – intsidenti esinemise tõenäosus;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 9) riskihaldus – vara, teabe, ohu, intsidenti 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 intsidente;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 10) haavatavuse analüüs – süsteemi üksikasjalik kontrollimine, et selgitada välja süsteemi turvanõrkused, ohud süsteemis töödeldava teabe salajasusele, terviklikkusele ja käideldavusele ning süsteemi vastuvõtlikkus mis tahes ründe või ohule;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 11) töötlussüsteemi turbejuhend – dokument, milles määratakse töötlussüsteemi tehnilisest lahendusest lähtudes kohustuslikud turvanõuded ning töötlussüsteemi eriõigustega kasutajate õigused ja kohustused töötlussüsteemi kasutamisel ning selle turvalisuse tagamisel;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 12) töötlussüsteemi kasutusjuhend – dokument, milles määratakse töötlussüsteemi turbejuhendis määratud kohustuslikest turvanõuetest lähtudes töötlussüsteemi kasutajate õigused ja kohustused töötlussüsteemi kasutamisel ning selle turvalisuse tagamisel;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 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;
- 16) paljastav kiirgus – töötlussüsteemist soovimatult kiirguv elektromagnetiline signaal, mis võimaldab ebaseaduslikku juurdepääsu teabele;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 17) kasutuslugu – töötlussüsteemi eesmärgi kirjeldus, millest selgub kes, millist teavet, kus ja kuidas töötleb;
[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- 18) kaasaskantav tööluseseade – töötlussüsteemiks või selle osaks olev seade, mida saab töötlussüsteemi teiste osadega füüsiliselt ühendamata kasutada töötlussüsteemis oleva teabe töötlemiseks.
[RT I, 29.12.2023, 8- jõust. 01.01.2024]

§ 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) [Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]
- (3¹) [Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]
- (4) Tööluseseadme, milles töötlemiseks lubatud kõrgeim teabe salastatuse tase on piiratud, võib viia väljapoole sisemist turvakeskkonda, kui:
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

1) salastatud teave on krüpteeritud nõuetele vastavate krüptomaterjalidega või kaitstud volitamata juurdepääsu eest muu Välisluureameti lubatud meetodiga;

[RT I, 06.10.2021, 1- jõust. 09.10.2021]

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 on ainult tööülesannete täitmiseks vajalikud kasutajaõigused – privileegide piiratuse põhimõte;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

4) eeldatakse kõigi süsteemiga ühendatud teiste süsteemide ebausaldusväärstust ning nendega teabe vahetamisel peab rakendama piisavaid turvameetmeid – isekaitsevate 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 teadmismisvajaduse 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 kasutajajooksul;

6) ära hoida ja kõrvaldada intsidente ning vältida või vähendada nende tekkimisega kaasnevat kahju;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

7) käsitleda intsidente, mille käigus määratakse kindlaks ja registreeritakse süsteemile või selle osale avaldunud oht ja selle tagajärjel teabele tekkinud kahju ning selle kõrvaldamiseks võetud meetmed.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2¹) Täpsemad nõuded töötlussüsteemile, sealhulgas sellega seotud töötlevatele üksustele ja selle kasutajatele, on esitatud lisas 14. Välisluureamet võib lähtuvalt turbehinnangust seada töötlussüsteemile täiendavaid nõudeid.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

(2²) Töötlev üksus võib rakendada lisas 14 esitatud nõuetest rangemaid nõudeid.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

(2³) Töötlev üksus võib lisas 14 esitatud nõuet rakendada osaliselt või jätta rakendamata erandina üksnes juhul, kui sellest tulenevad riskid on kirjeldatud töötlussüsteemi riskianalüüsis, seda kompenseerivad turvameetmed on kirjeldatud töötlussüsteemi turbejuhendis ja Välisluureamet on need töötlussüsteemi akrediteerimisel heaks kiitnud.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

(2⁴) Lisaks lõikes 2³ sätestatule võib töötlev üksus jätta lisas 14 esitatud nõude rakendamata juhul, kui rakendamine on töötlussüsteemi väiksuse või ülesehituse tõttu võimatu, seda on kirjeldatud töötlussüsteemi turbejuhendis ja Välisluureamet on selle töötlussüsteemi akrediteerimisel heaks kiitnud.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

(2⁵) Kui lisas 14 esitatud nõude rakendamine nõuab töötlevalt üksuselt regulaarseid toiminguid, peab nende sagedus olema kirjeldatud töötlussüsteemi turbejuhendis ning vastama töötlussüsteemi kasutusintensiivsusele.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

(3) Töötlussüsteemi kohta käiv teave dokumenteeritakse töötlussüsteemi turbejuhendis ja töötlussüsteemi kasutusjuhendis.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(4) Töötlussüsteemiga seotud töötlevad üksused teostavad oma ülesannete ulatuses pidevat töötlussüsteemi riskihaldust.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 106¹. Töötlussüsteemiga seotud töötlevad üksused

- (1) Töötlussüsteemi eest vastutav töötlev üksus (edaspidi *vastutav üksus*):
- 1) vastutab töötlussüsteemi haldamise seaduslikkuse ning töötlussüsteemi ja selles töödeldava teabe turvalisuse tagamise eest;
 - 2) korraldab töötlussüsteemi arendamist vastavalt kasutava üksuse vajadustele;
 - 3) planeerib vahendid töötlussüsteemi haldamiseks ja arendamiseks;
 - 4) otsustab kasutatavate üksuste töötlussüsteemiga liitumise üle;
 - 5) koostab koostöös haldava ja kasutava üksusega töötlussüsteemi riskianalüüsi ning hindab regulaarselt selle ajakohasust.
- (2) Töötlussüsteemi haldav töötlev üksus (edaspidi *haldav üksus*):
- 1) haldab töötlussüsteemi;
 - 2) arendab töötlussüsteemi tehnilist lahendust vastavalt vastutava üksuse suunistele;
 - 3) tagab töötlussüsteemi tehnilise lahenduse toimimise;
 - 4) tagab töötlussüsteemi ja selles töödeldava teabe turvalisuse ning kontrollib regulaarselt turvameetmete toimimist.
- (3) Töötlussüsteemi kasutav töötlev üksus (edaspidi *kasutav üksus*):
- 1) töötleb töötlussüsteemis tema valduses olevat teavet;
 - 2) esitab vastutavale üksusele töötlussüsteemi kasutamise ja arendamise vajadused;
 - 3) tagab oma asukohapunktis töötlussüsteemi ja selles töödeldava teabe turvalisuse, arvestades riskianalüüsis määratud turvariske, nende vastuvõetavaid piire ja turvameetmeid.
- (4) Lõigetes 1–3 loetletud ülesandeid võib täita sama töötlev üksus, tingimusel et rollide lahusus on töötlussüsteemi turbejuhendis kirjeldatud ja sisemise töökorraldusega tagatud.
- (5) Ühe töötlussüsteemi vastutava üksuse ülesandeid ei või täita mitu töötlevat üksust.
- (6) Ühel töötlussüsteemil võib olla mitu haldavat üksust ja kasutavat üksust.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 106². Töötlussüsteemi eest vastutav eriõigustega kasutaja

- (1) Töötlussüsteemi eest vastutaval eriõigustega kasutajal peab olema vähemalt töötlussüsteemis töödeldava teabe kõrgeimale salastatuse tasemele vastav juurdepääsuõigus.
- (2) Salastatud välisteabe töötlemiseks akrediteeritud töötlussüsteemi eest vastutava eriõigustega kasutaja puhul tuleb lisaks lõikes 1 sätestatule arvestada salastatud välisteabe avaldaja esitatud nõudeid.
- (3) Töötlussüsteemi eest vastutavad eriõigustega kasutajad määrab töötleva üksuse juht või tema volitatud isik kirjalikult.
- (4) Töötlussüsteemi eest vastutava eriõigustega kasutaja määramisest või vahetumisest teavitatakse viivitamata kirjalikult Välisluureametit ning Kaitsepolitsei ametit. Üks julgeolekuasutus ei teavita süsteemi eest vastutava eriõigustega kasutaja määramisest või vahetumisest teist julgeolekuasutust.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

§ 106³. Juurdepääs töötlussüsteemile

- (1) Töötlussüsteemi kasutaja võib olla teise töötleva üksuse juurdepääsuõiguse ja teadmismajadusega töötaja või ametnik, kui see on vajalik teise töötleva üksuse ülesannete täitmiseks.
- (2) Töötlussüsteemi osad võivad asuda teise töötleva üksuse otseses valduses ning töötlussüsteemi eest vastutav eriõigustega kasutaja võib olla teise töötleva üksuse töötaja või ametnik, kui on tagatud § 106 lõikes 2 ja lisas 14 sätestatud nõuete täitmine.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

§ 107. Töötlussüsteemi turbejuhend

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

- (1) Töötlussüsteemi turbejuhendis esitatakse:
- 1) töötlussüsteemi ja selles töödeldava teabe üldine kirjeldus;
 - 2) vastutav üksus, haldavad üksused ja kasutavad üksused;
 - 3) töötlussüsteemi eest vastutavate eriõigustega kasutajate ülesanded, õigused ja kohustused;

- 4) töötlussüsteemi turvalisuse korraldamise kirjeldus;
- 5) töötlussüsteemi tehniline kirjeldus, sealhulgas tehniline teave töötlussüsteemi ühenduste kohta teiste süsteemidega;
- 6) töötlussüsteemi riist- ja tarkvara loetelu, konfiguratsioon ja nende halduse kirjeldus;
- 7) töötlussüsteemile esitatavate turvanõuete kirjeldus, ülevaade töötlussüsteemi riskianalüüsi tulemustest ning neist lähtuvate turvameetmete loetelu.

(2) Töötlussüsteemi turbejuhendi töötab välja vastutav üksus koostöös haldava üksusega ja selle kehtestab vastutava üksuse juht. Enne kehtestamist kooskõlastab vastutav üksus töötlussüsteemi turbejuhendi Välisluureametiga.

(3) Töötlussüsteemi turbejuhendit täpsustatakse töötlussüsteemi ehitamise ja kasutamise käigus, juhul kui tehakse muudatusi, näiteks kui muudetakse töötlussüsteemi või selle osa kasutusotstarvet, ülesehitust, füüsilist asukohta, töötlussüsteemi riist- või tarkvaras tehakse suuremahulisi muudatusi, ilmnevad uued olulised ohud või muudetakse töötlussüsteemis töödeldava salastatud teabe taset. Töötlussüsteemi turbejuhendi muudatused kooskõlastab vastutav üksus Välisluureametiga.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 108. Töötlussüsteemi kasutusjuhend

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Töötlussüsteemi kasutusjuhendis esitatakse:

- 1) töötlussüsteemi lühikirjeldus;
- 2) töötlussüsteemi kasutajad ning nende ülesanded, õigused ja kohustused;
- 3) salastatud teabe elektroonilise töötlemise juhised;
- 4) töötlussüsteemis kasutatavate teabekandjate töötlemise kirjeldus;
- 5) töötlussüsteemi intsidentide haldamise ja ohuolukorras tegutsemise kirjeldus.

(2) Töötlussüsteemi kasutusjuhendi töötab töötlussüsteemi turbejuhendist lähtudes välja vastutav üksus koostöös haldava üksusega ja selle kehtestab vastutava üksuse juht. Enne kehtestamist kooskõlastab vastutav üksus töötlussüsteemi kasutusjuhendi Välisluureametiga.

(3) Töötlussüsteemi kasutusjuhendit täpsustatakse töötlussüsteemi kasutamise käigus, juhul kui tehakse muudatusi, näiteks kui muudetakse töötlussüsteemi või selle osa kasutusotstarvet, ülesehitust, füüsilist asukohta, töötlussüsteemi riist- või tarkvaras tehakse suuremahulisi muudatusi, ilmnevad uued olulised ohud või muudetakse töötlussüsteemis töödeldava salastatud teabe taset. Töötlussüsteemi kasutusjuhendi muudatused kooskõlastab vastutav üksus Välisluureametiga.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 109. Töötlussüsteemi akrediteerimine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Töötlussüsteemi akrediteerimise eesmärk on veenduda, et töötlussüsteem vastab elektroonilise teabeturbe tagamiseks kehtestatud nõuetele.

(2) Töötlussüsteemi akrediteerimise käigus Välisluureamet:

- 1) tutvub vastutava üksuse esitatud töötlussüsteemi eesmärgi ja kasutuslugudega;
- 2) vaatab üle töötlussüsteemi riskianalüüsi protsessi ja tulemused ning teeb kindlaks, et vastutav üksus on jääkriskid tuvastanud ja aktsepteerinud;
- 3) hindab töötlussüsteemi ülesehituse ning välimise, sisemise ja elektroonilise turvakeskkonna vastavust nõuetele;
- 4) hindab töötlussüsteemi turbejuhendit, töötlussüsteemi kasutusjuhendit ja muid töötlussüsteemi turvalisust puudutavaid dokumente;
- 5) hindab turvameetmete rakendamise ning töötlussüsteemi turvalisust puudutavate protseduuride vastavust nõuetele;
- 6) annab üldise turbehinnangu, mis väljendab töötlussüsteemis teabe kaitstuse vastavust nõuetele ja nende rakendamise hetkeseisu.

(3) Välisluureamet algatab töötlussüsteemi akrediteerimise vastutava üksuse taotlusel või omal algatusel. Vastutav üksus lisab töötlussüsteemi akrediteerimise taotlusele töötlussüsteemi turbejuhendi ja töötlussüsteemi kasutusjuhendi. Lõike 2 punktides 1–3, 5 ja 6 nimetatud teabe esitab vastutav üksus Välisluureameti nõudmisel.

(4) Töötlussüsteemi akrediteerimise tulemusena antakse töötlussüsteemile Välisluureameti peadirektori käskkirjaga vastavussertifikaat, kui:

- 1) töötlussüsteem vastab elektroonilise teabeturbe nõuetele või
- 2) töötlussüsteem ei vasta kõigile elektroonilise teabeturbe nõuetele, kuid sellest tingitud turvariskid on kompenseerivate turvameetmete tõttu püsivalts vastuvõetavad.

(5) Töötlussüsteemi akrediteerimise tulemusena antakse töötlussüsteemile Välisluureameti peadirektori käskkirjaga ajutine kasutusluba, kui töötlussüsteem ei vasta kõigile elektroonilise teabeturbe nõuetele, kuid sellest tingitud turvariskid on ajutiselt vastuvõetavad.

(6) Töötlussüsteemile, mida on vaja enne kasutusele võtmist testida, võib Välisluureameti peadirektori käskkirjaga väljastada testimiseks ajutise kasutusloa (edaspidi *testimisloa*). Testimisloa alusel võib töötlussüsteemi kasutada ja salastatud teavet töödelda üksnes töötlussüsteemi tehnilise lahenduse ja töötlussüsteemi ühenduste testimiseks. Testimisloa saamiseks peab vastutav üksus esitama töötlussüsteemi turbejuhendi ja töötlussüsteemi kasutusjuhendi üksnes nende olemasolu korral. Testimisloas määratakse töötlussüsteemi testimise tingimused, näiteks testimise eesmärk ja ulatus, testimise ajal töödelda lubatud teabe salastatuse tase ning testimise tähtaeg.

(7) Uue töötlussüsteemi ehitamise ja kasutusele võtmise korral võib töötlev üksus esitada taotluse koos planeeritava töötlussüsteemi ülesehituse lühikirjeldusega, misjärel väljastatakse ajutine kasutusloa üksnes töötlussüsteemi turbejuhendi ja töötlussüsteemi kasutusjuhendi koostamiseks.

(8) Välisluureamet keeldub peadirektori käskkirjaga töötlussüsteemile vastavussertifikaati või ajutist kasutusloa väljastamast ning keelab selle kasutamise salastatud teabe töötlemiseks, kui töötlussüsteem ei vasta elektroonilise teabeturbe nõuetele ja sellest tingitud turvariskid ei ole vastuvõetavad.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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. Töötlussüsteemi uuesti akrediteerimine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Töötlussüsteemi uuesti akrediteerimiseks esitab vastutav üksus taotluse:

- 1) vähemalt kaks kuud enne senise vastavussertifikaadi kehtivuse lõppemist;
- 2) vähemalt viis tööpäeva enne senise ajutise kasutusloa kehtivuse lõppemist.

(2) Kui uuesti akrediteerimise taotlus koos asjaomase dokumentatsiooniga on enne senise vastavussertifikaadi või ajutise kasutusloa kehtivuse lõppemist esitatud, võib Välisluureamet senise vastavussertifikaadi või ajutise kasutusloa kehtivust kuni akrediteerimise lõpuni pikendada.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 112. Vastavussertifikaadi ja ajutise kasutusloa kehtetuks tunnistamine

(1) Välisluureamet tunnistab vastavussertifikaadi või ajutise kasutusloa kehtetuks:

1) vastutava üksuse taotluse alusel;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2) kui vastutav, haldav või kasutav üksus ei ole täitnud Välisluureameti ettekirjutust elektroonilise teabeturbe nõude rikkumise või rikkumise ohu kõrvaldamiseks;

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

3) ilmneb vastavussertifikaadi või ajutise kasutusloa andmisest keeldumise aluseks olev asjaolu.

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

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

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 112¹. Salvestuskandjate hoiustamine kehtiva vastavussertifikaadi või ajutise kasutusloa puudumisel

Kehtiva vastavussertifikaadi või ajutise kasutusloa puudumisel peavad töötlussüsteemiga seotud töötlevad üksused tagama töötlussüsteemi osaks olnud salvestuskandjate ja nendes sisalduva teabe nõuetekohase hoiustamise.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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 töötlemisele kohaldatakse välislepingust tulenevaid või rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni salastatud teabe kaitse nõudeid, arvestades käesolevas jaos sätestatud. Käesolevas jaos sätestatud töötlemisnõudeid ei kohaldata Välisluureametis arvele võetud krüptomaterjalile ning «Riigisaladuse ja salastatud välisteabe seaduse» § 52 lõikes 3 nimetatud teabele.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 115. Salastatud välisteabe arvestus

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

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

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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 täiesti salajasel tasemel salastatud välisteabe ja erimärgistusega salastatud välisteabe kandjad.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 täiesti salajasel tasemel salastatud välisteavet ja 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.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(2) [Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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 täiesti salajasel tasemel salastatud välisteavet ja erimärgistusega salastatud välisteavet sisaldavale teabekandjale.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 118¹. Salastatud välisteavet sisaldava teabekandja märgistamine

(1) Salastatud välisteavet sisaldavale teabekandjale tehakse salastatud välisteabe avaldaja salastatuse taseme märgi, kui see on välislepinguga ette nähtud, ja sellele vastava taseme riigisaladuse märgi.

(2) Kui teabekandja sisaldab nii riigisaladust kui ka salastatud välisteavet, mille salastatuse tase on riigisaladuse salastatuse tasemest madalam, ei tehta sellele lõikes 1 nimetatud märget.

(3) Salastatud välisteavet sisaldavale teabekandjale tehakse lisamärke „Salastatud välisteave“ suurtähtedega ning märgitakse salastatud välisteabe avaldaja nimi, salastatuse tase ja salastamistähtaeg, kui välisteabe avaldaja on selle märkinud. Kui välisteabe avaldaja ei ole tähtaega märkinud, tehakse märged „tähtaeg: määramata“ või „tähtaeg: tähtajatu“. Sellisel juhul kehtib salastatus, kuni välisteabe avaldaja ei ole teatanud teisiti.

(4) Kui teabekandja sisaldab mitme avaldaja salastatud välisteavet, tuleb lõikes 3 sätestatud lisamärkes märkida kõik salastatud välisteabe avaldajad, salastatuse tasemed ja salastamistähtajad.

(5) Euroopa Liidu ja Põhja-Atlandi Lepingu Organisatsiooni salastatud välisteavet sisaldava teabekandja võib jätta lõigetes 1–4 sätestatud nõuete kohaselt märgistamata.

(6) Riigi julgeoleku volitatud esindaja kirjalikul nõusolekul võib elektroonilise salastatud välisteabe jätta lõigetes 1–4 sätestatud nõuete kohaselt märgistamata, kui teave on märgistatud §-s 70 sätestatud korras.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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, kui selline nõue tuleneb välislepingust.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(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

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 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.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 122¹. Salastatud teabe töötlemist eeldavad lepingud

(1) Tsiviilõiguslik leping, mille täitmine eeldab salastatud välisteabe töötlemist või riigisaladuse edastamist välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile, peab sisaldama osa, millega lepitakse kokku vähemalt selles, kelle loodud ning millisel tasemel salastatud teavet töödeldakse ning millised on juhised teabe kaitsmiseks, arvestades käesolevast määrusest ja välislepingutest tulenevaid nõudeid.

(2) Lõikes 1 nimetatud lepingu osa kooskõlastatakse enne lepingu sõlmimist riigi julgeoleku volitatud esindajaga.

(3) Ühe kuu jooksul lepingu sõlmimisest tuleb riigi julgeoleku volitatud esindajale esitada koopia selle lõikes 1 nimetatud osast, samuti lepingu poolte nimed, registrikoodid, asukohariigid ning lepingu kehtivusaeg.

(4) Lõikeid 2 ja 3 ei kohaldata „Riigisaladuse ja salastatud välisteabe seaduse“ § 52 lõikes 3 sätestatud juhul.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 122². Rahvusvahelise külastustaotluse kinnitamine

Rahvusvahelise külastustaotluse kinnitab riigi julgeoleku volitatud esindaja, välja arvatud „Riigisaladuse ja salastatud välisteabe seaduse“ § 52 lõikes 3 sätestatud juhul.
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

2. jaotis

Euroopa Liidu ja Põhja-Atlandi Lepingu Organisatsiooni salastatud välisteabele juurdepääsu ja töötlemise õiguse andmise, sellest keeldumise, selle pikendamise ja kehtetuks tunnistamise kord

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 123. Euroopa Liidu ja Põhja-Atlandi Lepingu Organisatsiooni salastatud välisteabele juurdepääsu õigus ja selle töötlemise õigus

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Euroopa Liidu ja Põhja-Atlandi Lepingu Organisatsiooni piiratud tasemel salastatud välisteabele juurdepääsu õiguse saamise eeltingimus „Riigisaladuse ja salastatud välisteabe seaduse“ § 27 lõikes 1, 2 või 5 nimetatud isikul on §-s 130 nimetatud tutvustuse läbimine ja kohustuse allkirjastamine.

(2) Euroopa Liidu ja Põhja-Atlandi Lepingu Organisatsiooni konfidentsiaalsel ja kõrgemal tasemel salastatud välisteabele juurdepääsu õigus on füüsilisel isikul juurdepääsusertifikaadi alusel.

(3) Euroopa Liidu ja Põhja-Atlandi Lepingu Organisatsiooni piiratud ja kõrgemal tasemel salastatud välisteabe töötlemise õigus on isikul töötlemiseks mõeldud juurdepääsusertifikaadi (edaspidi *töötlemissertifikaat*) alusel.

(4) Juurdepääsusertifikaadi saamise eeltingimus on riigisaladusele juurdepääsu luba ning töötlemissertifikaadi saamise eeltingimus on riigisaladuse töötlemisluba.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 124. Juurdepääsusertifikaadi ja töötlemissertifikaadi tasemete vastavus

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

Isikule ei anta:

1) kõrgemal tasemel salastatud välisteabele juurdepääsu sertifikaati, kui on tema riigisaladusele juurdepääsu loa tase;

2) kõrgemal tasemel salastatud välisteabe töötlemissertifikaati, kui on tema riigisaladuse töötlemisloa tase.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 125. Juurdepääsusertifikaadi ja töötlemissertifikaadi kehtivus

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Juurdepääsu- või töötlemissertifikaadi kehtivusaja otsustab riigi julgeoleku volitatud esindaja vastavalt taotluses märgitud soovitava kehtivusperioodile, juurdepääsuloa või töötlemisloa kehtivusele ja juurdepääsuvajaduse põhjendatusele. Kui välislepingust tulenevad juurdepääsuõiguse andmisest keeldumise alused on rangemad võrreldes „Riigisaladuse ja salastatud välisteabe seaduses“ sätestatud alustega, võetakse juurdepääsu- või töötlemissertifikaadi kehtivusaja otsustamisel arvesse ka välislepingust tuleneva asjaolu esinemist.

(2) Juhul, kui isiku riigisaladusele juurdepääsu luba või töötlemisluba lõppeb enne juurdepääsu- või töötlemissertifikaadi kehtivusaja lõppu, kaotab juurdepääsu- või töötlemissertifikaat kehtivuse.

(3) Kui juurdepääsu- või töötlemissertifikaat kaotab kehtivuse enne oma kehtivusaja lõppu, tuleb see tagastada riigi julgeoleku volitatud esindajale.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 126. Juurdepääsusertifikaadi taotlemine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Juurdepääsusertifikaadi taotlemiseks esitab riigiasutus, Eesti Pank või Kaitseliit, kelle ülesannete tõttu tekib isikul juurdepääsuvajadus, või selleks volitatud asutus (edaspidi *taotleja*) riigi julgeoleku volitatud esindajale:

1) kirjaliku taotluse, milles märgitakse salastatud välisteabe avaldaja ja salastatuse tase, millele juurdepääsu taotletakse, juurdepääsusertifikaadi taotletav kehtivusaeg, samuti isiku nimi, isikukood, sünnikoht, kodakondsus, kontaktandmed ja ametikoht;

2) isiku juurdepääsuloa või muu riigisaladusele juurdepääsu õigust kinnitava dokumendi või selle koopia, välja arvatud juhul, kui taotleja on julgeolekuasutus.

[RT I, 29.12.2023, 8- jõust. 01.01.2024]

(2) „Riigisaladuse ja salastatud välisteabe seaduse“ § 30¹lõikes 1 nimetatud isikule juurdepääsusertifikaadi taotlemiseks esitab Kaitseväge riigi julgeoleku volitatud esindajale ametikohtade loetelu, milles on märgitud iga ametikoha kohta selleks nõutava salastatud välisteabele juurdepääsu õiguse tase.

(3) Lõikes 2 nimetatud isikute juurdepääsusertifikaatide taotlemiseks esitab riigi julgeoleku volitatud esindajale riigiasutus, kelle põhiülesanne on koordineerida ja korraldada reservteenistusega seotud tegevusi ja arvestuse pidamist:

- 1) teabe sõjaväelise auastmega sõjaaja ametikohale isiku nimetamise kohta;
- 2) taotletava juurdepääsusertifikaadi kehtivusaja, samuti isiku nime, isikukoodi, sünnikoha, kodakondsuse ja kontaktandmed;
- 3) teabe isikule riigisaladusele juurdepääsu andmise õiguse andmise ja kehtivuse kohta.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 127. Piiratud tasemel salastatud välisteabele juurdepääsu õiguse taotlemine

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 128. Töötlemisertifikaadi taotlemine

Töötlemisertifikaadi taotlemiseks peab taotleja esitama riigi julgeoleku volitatud esindajale järgmised dokumendid:

- 1) taotleja kirjalik taotlus, milles nimetatakse salastatud välisteabe avaldaja ja välisteabe salastatuse tase, millele juurdepääsu taotletakse, ning põhjendatakse isiku salastatud välisteabele juurdepääsu vajadust;
- 2) töötlemisloa koopia;
- 3) salastatud teabe kaitse juhendi koopia;
- 4) koopia dokumendist, millega määratakse nimeliselt juriidilise isiku riigisaladuse kaitset korraldava isik, samuti nende isikute nimekiri, kes hakkavad salastatud välisteavet töötleva, ning vajaduse korral dokumendid neile füüsilise isiku juurdepääsusertifikaadi taotlemiseks.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 129. Juurdepääsusertifikaadi ja töötlemisertifikaadi andmise otsustamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Kui juurdepääsu- või töötlemisertifikaadi andmise taotlus või sellele lisatud dokumendid ei vasta nõuetele, annab riigi julgeoleku volitatud esindaja taotlejale kümne tööpäeva jooksul teada puudustest ja määrab tähtaja nende kõrvaldamiseks.

(2) Juurdepääsu- või töötlemisertifikaadi andmise või sellest keeldumise otsustab riigi julgeoleku volitatud esindaja ühe kuu jooksul nõuetekohase taotluse saamisest. Põhjendatud vajaduse korral võib tähtaega pikendada, teavitades sellest taotlejat.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 130. Salastatud välisteabe kaitse nõuete tutvustamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Enne esmakordset piiratud tasemel salastatud välisteabele juurdepääsu õiguse või juurdepääsusertifikaadi andmist ning vajaduse korral ka juurdepääsuõiguse või juurdepääsusertifikaadi korduval andmisel tutvustatakse isikule salastatud välisteabe kaitse aluseid. Tutvustuse korraldab:

- 1) juurdepääsusertifikaadi andmise korral riigi julgeoleku volitatud esindaja või volitatud asutus;
- 2) piiratud tasemel salastatud välisteabele juurdepääsu õiguse andmise korral riigiasutus, Eesti Pank või Kaitseliit, mille töö- või ametikohal isik töötab või mille juhi otsuse alusel on tal juurdepääsuõigus.

(2) Salastatud välisteabe kaitse alustega tutvumise järel kinnitab isik lisas 13 toodud vormil allkirjaga, et on teadlik salastatud välisteabe kaitse nõuetest, vastutusest nende rikkumise eest ja kohustusest hoida temale teatavaks saavat salastatud välisteavet.

(3) Lõikes 1 nimetatud tutvustuse korraldaja säilitab lõikes 2 nimetatud kinnitust salastatud välisteabele juurdepääsu õiguse või juurdepääsusertifikaadi kehtivuse ajal ning vähemalt viis aastat pärast selle lõppemist.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 131. Juurdepääsusertifikaadi ja töötlemisertifikaadi edastamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

Riigi julgeoleku volitatud esindaja edastab juurdepääsu- või töötlemisertifikaadi viie tööpäeva jooksul taotlejale.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 132. Juurdepääsusertifikaadi ja töötlemisertifikaadi vormistamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

(1) Juurdepääsu- või töötlemisertifikaadil peavad olema vähemalt järgmised andmed:

- 1) väljaandmise kuupäev ja number;
- 2) juurdepääsu- või töötlemisertifikaadi saanud füüsilise isiku ees- ja perekonnanimi, sünniaeg, isikukood, sünnikoht ja kodakondsus või juriidilise isiku nimi, aadress ja registrikood;
- 3) salastatud välisteabe kõrgeim tase ja erikategooriad, millele juurdepääsu või mille töötlemise õigus isikule antakse;
- 4) kehtivusaeg.

(2) Juurdepääsusertifikaat ja töötlemisertifikaat vormistatakse inglise ja eesti keeles.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 133. Kinnituse taotlemine ja vormistamine

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 134. Juurdepääsusertifikaadi ja töötlemisertifikaadi kehtetuks tunnistamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

Juurdepääsu- või töötlemisertifikaat tunnistatakse kehtetuks:

- 1) isiku juurdepääsuvajaduse äralangemisel;
- 2) uue juurdepääsu- või töötlemisertifikaadi väljastamisel enne eelmise juurdepääsu- või töötlemisertifikaadi kehtivusaja lõppu;
- 3) juurdepääsu- või töötlemisertifikaadile kantud isikuandmete muutumisel;
- 4) kui väljastatud juurdepääsu- või töötlemisertifikaadi kehtivusajal ilmneb mõni selle väljastamist välistav asjaolu.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 135. Juurdepääsu- ja töötlemisertifikaadi andmise aluseks olnud andmete muutmisest teavitamine

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

Taotleja teavitab viivitamata riigi julgeoleku volitatud esindajat juurdepääsuõiguse saanud isiku salastatud välisteabele juurdepääsu vajaduse või riigisaladusele juurdepääsu loa või õiguse või töötlemisloa lõppemisest ning § 134 punktides 3 ja 4 nimetatud sündmusest.

[RT I, 31.05.2023, 3- jõust. 05.06.2023]

§ 136. Julgeolekukontrolli teostamiseks pädeva asutuse teavitamine

[Kehtetu -RT I, 31.05.2023, 3- jõust. 05.06.2023]

6. peatükk

NÕUSOLEKU, KINNITUSE, JUURDEPÄÄSULOJA JA TÖÖTLEMISLOA NING NENDE KEHTIVUSE PIKENDAMISE TAOTLUSE, JUURDEPÄÄSULOJA JA TÖÖTLEMISLOA TAOTLEJA JA PIKENDAJA ANKEEDI VORMIDE KEHTESTAMINE

§ 137. Riigisaladusele juurdepääsu loa vormid

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

(2) Füüsiline isik esitab juurdepääsuloa kehtivuse pikendamise lisa 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. Riigisladuse töötlemisloa vormid

- (1) Juriidiline isik esitab riigisladuse töötlemisloa (edaspidi *töötlemisluba*) taotluse lisa 7 toodud vormil.
- (2) Juriidiline isik esitab töötlemisloa kehtivuse pikendamise taotluse lisa 8 toodud vormil.
- (3) Juriidiline isik esitab töötlemisloa taotlemisel või töötlemisloa kehtivuse pikendamise taotlemisel töötlemisloa taotleja ja pikendaja ankeedi (lisa 9).
[RT I, 06.03.2019, 7- jõust. 09.03.2019]
- (4) [Kehtetu -RT I, 06.03.2019, 7- jõust. 09.03.2019]
- (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 riigisladuse kaitse nõuetest, vastutusest nende rikkumise eest ja kohustusest hoida temale teatavaks saavat riigisladust (lisa 12).
- (7) Lõikeid 1–3, 5 ja 6 kohaldatakse ka füüsilisest isikust ettevõtjale.
[RT I, 06.03.2019, 7- jõust. 09.03.2019]

7. peatükk MÄÄRUSE RAKENDAMINE

§ 138¹. Määruse rakendamine

- (1) Enne 5. juunit 2023. a käesoleva määruse § 6 lõike 1 punkti 2 alusel salastatud teave jääb riigisladuseks vastavalt salastamise ajal kehtinud nõuetele.
- (2) Enne 5. juunit 2023. a kehtestatud riigisladuse kaitse juhend viiakse käesoleva määruse nõuetega kooskõlla hiljemalt 1. oktoobriks 2023. a.
- (3) Alates 5. juunist 2023. a kehtivaid nõudeid registrisse kantavale teabele kohaldatakse teabekandjale, mis registreeritakse alates 5. juunist 2023. a.
- (4) Arhiivihoidlas olev teabekandja viiakse kooskõlla 5. juunist 2023. a kehtivate märgistamise nõuetega teabekandja töötlemisel, välja arvatud vahetult hoidmise ja säilitamisega seotud toimingud, kuid hiljemalt 1. juuniks 2028. a.
- (5) Enne 5. juunit 2023. a töötlussüsteemile antud vastavussertifikaat või ajutine kasutusluba kehtib selle kehtivuse tähtaja lõpuni.
- (6) Enne 5. juunit 2023. a füüsilisele isikule või töötlemisloa alusel salastatud teavet töötlevale isikule antud juurdepääsusertifikaat kehtib selle kehtivusaja lõpuni.
- (7) Töötlussüsteemi turbejuhend ja töötlussüsteemi kasutusjuhend tuleb viia §-des 107 ja 108 sätestatuga kooskõlla hiljemalt järgmise akrediteerimise ajaks.
- (8) Enne 5. juunit 2023. a soetatud salastatud teabekandja hävitamise seadet, mis ei vasta käesoleva määruse § 83 nõuetele, võib kasutada järgmiselt:
 - 1) paberipurustajat kuni 30. aprillini 2026. a;
 - 2) Välisluureametiga kooskõlastatud salvestuskandja hävitamise seadet selle elutsükli lõpuni.[RT I, 31.05.2023, 3- jõust. 05.06.2023]
- (9) Vastutava üksuse infoturbejuhi ülesandeid täitev isik peab vastama § 23 lõikes 3 sätestatud nõudele hiljemalt 1. jaanuaril 2025. a.
[RT I, 29.12.2023, 8- jõust. 01.01.2024]

§ 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 ja töötlemisloa kehtivusaja pikendaja ankeet
[RT I, 06.03.2019, 7- jõust. 09.03.2019]

[Lisa 10](#) Riigisaladuse töötlemisloa pikendaja ankeet
[Kehtetu -RT I, 06.03.2019, 7- jõust. 09.03.2019]

[Lisa 11](#) Juriidilise isiku riigisaladuse töötlemisloa või selle kehtivuse pikendamise taotleja kirjalik nõusolek
[RT I, 06.03.2019, 7- jõust. 09.03.2019]

[Lisa 12](#) Juriidilise isiku kinnitus hoida teatavaks saavat riigisaladust

[Lisa 13](#) Füüsilise isiku kinnitus hoida teatavaks saavat salastatud välisteavet
[RT I, 31.05.2023, 3- jõust. 05.06.2023]

[Lisa 14](#) Nõuded salastatud teabe töötlussüsteemile
[RT I, 29.12.2023, 8- jõust. 01.01.2024]