KOMISIJOS SPRENDIMAS (ES) 2022/640

2022 m. balandžio 7 d.

dėl įgyvendinimo taisyklių, susijusių su pagrindinių saugumo subjektų funkcijomis ir atsakomybe

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 249 straipsnį,

atsižvelgdama į 2015 m. kovo 13 d. Komisijos sprendimą (ES, Euratomas) 2015/443 dėl saugumo Komisijoje ([1]),

atsižvelgdama į 2015 m. kovo 13 d. Komisijos sprendimą (ES, Euratomas) 2015/444 dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių ([2]),

kadangi:

(1) sprendimai (ES, Euratomas) 2015/443 ir (ES, Euratomas) 2015/444 taikomi visiems Komisijos padaliniams ir patalpoms;

(2) prireikus pagal Sprendimo (ES, Euratomas) 2015/444 60 straipsnį turi būti priimtos įgyvendinimo taisyklės, skirtos tam sprendimui papildyti ar sustiprinti;

(3) ES įslaptintos informacijos apsaugai užtikrinti skirtos saugumo priemonės visą savo gyvavimo ciklą turėtų visų pirma atitikti jos slaptumo žymos lygį;

(4) Komisijos sprendime (ES, Euratomas) 2017/46 ([3]), visų pirma jo 3 straipsnyje dėl Komisijos IT saugumo principų ir 9 straipsnyje dėl sistemų savininkų, nustatytos Komisijos ryšių ir informacinių sistemų apsaugos priemonės;

(5) įgyvendinimo taisyklių, susijusių su pagrindinių saugumo subjektų funkcijomis ir atsakomybe, tikslas – pateikti gaires dėl išankstinių sąlygų ir pareigų, kurios toms funkcijoms nustatytos sprendimuose (ES, Euratomas) 2015/443 ir (ES, Euratomas) 2015/444;

(6) Sprendimo (ES, Euratomas) 2015/444 36 straipsnio 7 dalyje nustatytos kelios papildomos su saugumu susijusios funkcijos, kurias turi vykdyti Komisijos saugumo institucija. Su šiomis funkcijomis susijusios užduotys nustatytos šiame sprendime;

(7) pagal Sprendimą (ES, Euratomas) 2015/444 vietos saugumo pareigūnams ir registracijos kontrolės pareigūnams tenka konkreti atsakomybė už ES įslaptintos informacijos apsaugą savo padaliniuose;

(8) 2016 m. gegužės 4 d. Komisija priėmė sprendimą ([4]), kuriuo už saugumo reikalus atsakingam Komisijos nariui suteikiami įgaliojimai Komisijos vardu ir jos atsakomybe patvirtinti įgyvendinimo taisykles, numatytas Sprendimo (ES, Euratomas) 2015/444 60 straipsnyje. Vėliau, 2021 m. balandžio 13 d., už saugumo reikalus atsakingas Komisijos narys Komisijos vardu ir jos atsakomybe priėmė sprendimą ([5]), kuriuo šios įgyvendinimo taisyklės perdeleguojamos Žmogiškųjų išteklių ir saugumo generalinio direktorato generaliniam direktoriui,

([1]) OL L 72, 2015 3 17, p. 41.
([2]) OL L 72, 2015 3 17, p. 53.
([3]) 2017 m. sausio 10 d. Komisijos sprendimas (ES, Euratomas) 2017/46 dėl Europos Komisijos ryšių ir informacinių sistemų saugumo (OL L 6, 2017 1 11, p. 40).
([4]) 2016 m. gegužės 4 d. Sprendimas C(2016) 2797 *final* dėl su saugumu susijusio įgaliojimo.
([5]) 2021 m. balandžio 13 d. Sprendimas C(2021) 2684 *final*, kuriuo perdeleguojami įgaliojimai, suteikti Komisijos sprendimu C(2016) 2797 dėl su saugumu susijusio įgaliojimo.

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 SKYRIUS

Bendrosios nuostatos

1 straipsnis

Dalykas ir taikymo sritis

1. Šiuo sprendimu nustatomos pagrindinių saugumo subjektų, kurie pagal sprendimus (ES, Euratomas) 2015/443 ir (ES, Euratomas) 2015/444 atsako už ES įslaptintos informacijos (toliau – ESĮI) apsaugą Komisijoje, funkcijos ir atsakomybė.

2. Šis sprendimas taikomas visiems Komisijos padaliniams ir visose Komisijos patalpose.

2 SKYRIUS

Žmogiškųjų išteklių ir saugumo generalinis direktoratas

2 straipsnis

Komisijos saugumo institucija

1. Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato direktorius atlieka Sprendimo (ES, Euratomas) 2015/444 7 straipsnyje nurodytos Komisijos saugumo institucijos (KSI) funkcijas.

2. Pagal šio sprendimo 3–7 straipsnius KSI savo funkcijas vykdo šiose Sprendimu (ES, Euratomas) 2015/444 nustatytose srityse:

a) personalo saugumo;

b) fizinio saugumo;

c) ESIĮ valdymo;

d) visų ryšių ir informacinių sistemų (RIS), kuriose tvarkoma ESĮI, akreditavimo;

e) pramoninio saugumo ir

f) keitimosi įslaptinta informacija.

3. KSI vietos saugumo pareigūnams (VSP), VSP pavaduotojams, registracijos kontrolės pareigūnams (RKP) ir RKP pavaduotojams rengia privalomus mokymus apie jų atsakomybę ir pareigas.

3 straipsnis

Informacijos saugumo užtikrinimo institucija

Informacijos saugumo užtikrinimo institucija atsako už šią su ESĮI apsauga susijusią veiklą:

a) informacijos saugumo užtikrinimo politikos ir saugumo gairių rengimą ir jų veiksmingumo bei tinkamumo stebėseną;

b) su kriptografinėmis priemonėmis susijusios techninės informacijos apsaugą ir administravimą;

c) užtikrinimą, kad, kai tikslinga, informacijos saugumo užtikrinimo priemonės atitiktų Komisijos saugumo ir viešųjų pirkimų politiką;

d) užtikrinimą, kad kriptografinės priemonės būtų pasirenkamos laikantis jų tinkamumo nustatymo ir atrankos politikos;

e) konsultacijas su sistemų savininkais, sistemų tiekėjais, saugumo subjektais ir naudotojų atstovais informacijos saugumo užtikrinimo politikos ir saugumo gairių klausimais.

4 straipsnis

Saugumo akreditavimo institucija

1. KSI atsako už Sprendimo 2015/444 18 straipsnio reikalavimus atitinkančių saugių zonų ir ESĮI tvarkyti skirtų RIS akreditavimą.

2. Komisijos padaliniai, derindami veiksmus su savo VSP ir, kai tinkama, su savo vietos informatikos saugumo pareigūnu (toliau – VISP), konsultuojasi su saugumo akreditavimo institucija, jei padalinys ketina:

a) kurti saugią zoną;

b) įdiegti ESĮI tvarkyti skirtą RIS;

c) įrengti bet kokią kitą įslaptintai informacijai tvarkyti skirtą įrangą, įskaitant jungtis su trečiosios šalies RIS.

Saugumo akreditavimo institucija teikia konsultacijas dėl šios veiklos vykstant tiek planavimo, tiek kūrimo ar plėtros procesams.

3. ESĮI saugioje zonoje arba RIS tvarkoma tik saugumo akreditavimo institucijai suteikus atitinkamo lygio ESĮI akreditaciją.

4. Saugios zonos akreditavimo reikalavimai apima:

a) saugios zonos planų patvirtinimą;

b) visų sutarčių dėl darbų, kuriuos atlieka išorės rangovai, patvirtinimą, atsižvelgiant į pramoninio saugumo nuostatas, pavyzdžiui, bet kokius reikalavimus dėl rangovų ir jų darbuotojų patikimumo pažymėjimų;

c) visų reikiamų deklaracijų ir atitikties sertifikatų pateikimą;

d) fizinį saugios zonos patikrinimą siekiant nustatyti, ar statybinės medžiagos ir metodai, prieigos kontrolė, saugumo įranga ir visi kiti objektai atitinka KSI nustatytus reikalavimus;

e) elektromagnetinei spinduliuotei taikytinų atsakomųjų priemonių bet kurioje techniniu požiūriu saugioje zonoje patvirtinimą;

f) saugios zonos saugios eksploatacijos taisyklių (SecOPs) patvirtinimą.

5. RIS, kuriose tvarkoma ESĮI, akreditavimo reikalavimai apima:

a) sistemos akreditavimo strategijos parengimą;

b) rizikos valdymo metodu paremto RIS saugumo plano patvirtinimą;

c) ryšių ir informacinėms sistemoms (RIS) taikytinų SecOPs patvirtinimą;

d) visų kitų reikalaujamų saugumo dokumentų, kuriuos nustato saugumo akreditavimo institucija, patvirtinimą;

e) bet kokio šifravimo technologijų naudojimo patvirtinimą;

f) RIS, kuriose tvarkoma CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta informacija, atveju elektromagnetinei spinduliuotei taikytinų atsakomųjų priemonių patvirtinimą;

g) RIS patikrinimą siekiant nustatyti, ar tinkamai įgyvendinamos dokumentais pagrįstos saugumo priemonės.

6. Sėkmingai įvykdžius akreditavimo reikalavimus, saugumo akreditavimo institucija, atsižvelgdama į tvarkomos ESĮI lygį ir susijusią riziką, išduoda oficialų leidimą tvarkyti ESĮI saugioje zonoje arba RIS nurodytu aukščiausiu tvarkomos ESĮI slaptumo žymos lygiu ir ne ilgiau kaip penkeriems metams.

7. Gavusi pranešimą apie saugumo pažeidimą arba esminį saugios zonos arba RIS struktūros ar saugumo priemonių pasikeitimą, saugumo akreditavimo institucija peržiūri ir prireikus gali atšaukti leidimą tvarkyti ESĮI, kol bus pašalinti visi nustatyti nesklandumai.

5 straipsnis

TEMPEST institucija

1. TEMPEST saugumo priemonės taikomos siekiant apsaugoti RIS, kuriose tvarkoma CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta informacija, ir gali būti taikomos slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėtai informacijai.

2. TEMPEST institucija atsako už priemonių, skirtų ESĮI apsaugoti nuo neteisėto atskleidimo dėl netyčinio elektromagnetinio spinduliavimo, patvirtinimą.

3. RIS, kuriose tvarkoma ESĮI, savininko prašymu TEMPEST institucija parengia TEMPEST saugumo priemonių specifikacijas, atitinkančias informacijos slaptumo žymos lygį.

4. Saugių zonų ir CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėtai ESĮI tvarkyti skirtų RIS akreditavimo metu TEMPEST institucija atlieka techninius bandymus ir, jei jie sėkmingi, išduoda TEMPEST sertifikatą.

5. TEMPEST sertifikate pateikiama bent ši informacija:

a) bandymo data;

b) TEMPEST saugumo priemonių aprašymas ir patalpų planai;

c) sertifikato galiojimo pabaigos data;

d) visi pakeitimai, dėl kurių sertifikatas tampa negaliojančiu;

e) TEMPEST institucijos parašas.

6. VSP arba susitikimo rengėjas, atsakingas už susitikimo, kuriame naudojama įslaptinta informacija, organizavimą, derindamas veiksmus su VSP, gali prašyti TEMPEST institucijos išbandyti susitikimų sales ir taip užtikrinti, kad techniniu požiūriu jos būtų saugios.

6 straipsnis

Kriptografijos patvirtinimo institucija

1. Kriptografijos patvirtinimo institucija atsako už šifravimo technologijų naudojimo patvirtinimą.

2. Kriptografijos patvirtinimo institucija parengia gaires dėl šifravimo technologijų naudojimo ir patvirtinimo reikalavimų.

3. Kriptografijos patvirtinimo institucija, remdamasi sistemos savininko prašymu, patvirtina šifravimo sprendimų naudojimą. Patvirtinimas grindžiamas patenkinamu bent šių aspektų vertinimu:

a) saugotinos informacijos saugumo poreikių;

b) su sprendimu susijusios RIS apžvalgos;

c) būdingos ir likutinės rizikos vertinimo;

d) siūlomo sprendimo aprašymo;

e) šifravimo sprendimo SecOPs.

4. Kriptografijos patvirtinimo institucija tvarko patvirtintų šifravimo sprendimų registrą.

7 straipsnis

Kriptografijos platinimo institucija

1. Kriptografijos platinimo institucija atsako už kriptografinės medžiagos, naudojamos ESĮI (daugiausia šifravimo įrangos, kriptografinių raktų, sertifikatų ir susijusių autentiškumo patvirtinimo priemonių) apsaugai, platinimą šiems naudotojams:

a) išorės šalių administruojamų RIS atveju – Komisijai priklausantiems naudotojams arba padaliniams;

b) Komisijos administruojamų RIS atveju – Komisijai nepriklausantiems naudotojams arba organizacijoms.

2. Pagal Sprendimo 2015/443 17 straipsnio 3 dalį atsakomybę už kriptografinės medžiagos platinimą trečiosioms šalims kriptografijos platinimo institucija gali perduoti kitiems padaliniams.

3. Kriptografijos platinimo institucija užtikrina, kad visa kriptografinė medžiaga būtų siunčiama saugiais kanalais, apsaugančiais nuo bet kokio klastojimo ir pateikiančiais klastojimo, jei tokio būta, įrodymus, laikantis ESĮI, kuri bus apsaugota ta medžiaga, slaptumo žymos lygiui taikomų saugumo taisyklių.

4. Kriptografijos platinimo institucija teikia gaires VSP ir, kai tinkama, kiekvieno Komisijos padalinio, dalyvaujančio kuriant, platinant ar naudojant kriptografinę medžiagą, vietos informatikos saugumo pareigūnui.

5. Kriptografijos platinimo institucija užtikrina, kad būtų nustatytos platinimo procesui tinkamos SecOPs.

3 SKYRIUS

Komisijos padaliniai

8 straipsnis

Padalinio vadovai

1. Kiekvienas padalinio vadovas skiria:

a) padaliniui arba kabinetui – VSP ir, kai tinkama, vieną ar daugiau jo pavaduotojų;

b) kiekvienam padaliniui, kuriame veikia ESĮI registratūra, – RKP ir, kai tinkama, vieną ar daugiau jo pavaduotojų;

c) kiekvienai RIS, kurioje tvarkoma ESĮI, – sistemos savininką.

2. Prieš paskirdamas VSP, VSP pavaduotojus, RKP ir RKP pavaduotojus, padalinio vadovas prašo Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato direktoriaus patvirtinimo.

3. Pasikonsultavęs su VSP, padalinio vadovas nustato visas pareigas, kurioms užimti reikalingas patikimumo patikrinimas, kad būtų galima susipažinti su ESĮI. Kandidatai į tokias pareigas informuojami apie tai, kad įdarbinimo proceso metu turi būti patikrintas jų patikimumas.

4. Bet kurio ESĮI turinčio padalinio vadovas atsako už sunaikinimo ir evakuacijos ekstremaliosios padėties atveju planų aktyvavimą, kai tai būtina. Planuose turi būti numatyta alternatyva tais atvejais, kai su padalinio vadovu susisiekti negalima.

9 straipsnis

RIS, kuriose tvarkoma ESĮI, savininkai

1. Kad įdiegtų RIS, kurioje tvarkoma ESĮI, ir nustatytų atitinkamus saugumo standartus bei reikalavimus ir pradėtų saugumo akreditavimo procesą, sistemos savininkas kuo ankstesniu projekto vykdymo etapu susisiekia su saugumo akreditavimo institucija.

2. Sistemos savininkas užtikrina, kad saugumo priemonės atitiktų saugumo akreditavimo institucijos reikalavimus ir kad ESĮI nebūtų tvarkoma RIS, kol ji nėra akredituota.

3. Sistemos savininkas, norėdamas gauti patvirtinimą naudoti bet kokias šifravimo technologijas, susisiekia su Kriptografijos patvirtinimo institucija. Sistemų savininkai nenaudoja šifravimo technologijų gamybos sistemose be išankstinio patvirtinimo.

4. Su RIS saugumu susijusiais klausimais sistemos savininkas konsultuojasi su padalinio VISP.

5. Sistemos savininkas bent kartą per metus peržiūri sistemai taikomas saugumo priemones, įskaitant jos saugumo planą.

6. Jei RIS įvyksta saugumo incidentas ir nurodoma, kad RIS nebegali tinkamai apsaugoti ESĮI, sistemos savininkas informuoja VSP ir nedelsdamas kreipiasi į saugumo akreditavimo instituciją, prašydamas patarimo dėl tolesnių veiksmų. Tokiu atveju, kol nebus imtasi tinkamų taisomųjų veiksmų, akreditavimo procesas gali būti sustabdytas ir sistemos eksploatavimas gali būti nutrauktas.

7. Sistemos savininkas visada teikia visapusišką paramą saugumo akreditavimo institucijai vykdant su RIS akreditavimu susijusias pareigas.

10 straipsnis

Informacijos saugumo užtikrinimo operacinė institucija

Kiekvienos RIS informacijos saugumo užtikrinimo operacinė institucija:

a) parengia saugumo dokumentus, atitinkančius saugumo politiką ir gaires, visų pirma saugumo planą, su sistema susijusias SecOPs ir RIS akreditavimo proceso kriptografinius dokumentus;

b) dalyvauja atrenkant ir bandant konkrečioms sistemoms skirtas techninio saugumo priemones, prietaisus ir programinę įrangą, siekiant prižiūrėti, kaip jie taikomi, ir užtikrinti, kad jie būtų saugiai įdiegti, sukonfigūruoti ir eksploatuojami pagal atitinkamus saugumo dokumentus;

c) dalyvauja atrenkant TEMPEST saugumo priemones ir prietaisus, jei to reikalaujama saugumo plane, ir, bendradarbiaudama su TEMPEST institucija, užtikrina, kad jie būtų saugiai įdiegti ir eksploatuojami;

d) stebi, kaip įgyvendinamos ir taikomos su sistemos eksploatavimu susijusios SecOPs;

e) bendradarbiaudama su Kriptografijos platinimo institucija, valdo ir tvarko kriptografines priemones, kad užtikrintų tinkamą kriptografinės medžiagos ir kontroliuojamų objektų saugojimą, o prireikus – kriptografinių kintamųjų generavimą;

f) atlieka saugumo analizę, peržiūras ir bandymus, visų pirma siekdama parengti atitinkamas rizikos ataskaitas, kurių reikalauja saugumo akreditavimo institucija;

g) rengia konkrečioms RIS skirtus informacijos saugumo užtikrinimo mokymus;

h) įgyvendina ir taiko konkrečioms RIS skirtas apsaugos priemones.

4 SKYRIUS

Vietos saugumo pareigūnas

11 straipsnis

VSP paskyrimas

1. VSP ir VSP pavaduotojai yra pareigūnai arba laikinieji darbuotojai.

2. Visi VSP ir VSP pavaduotojai turi turėti galiojantį saugumo leidimą susipažinti su iki SECRET UE/ES SECRET lygio slaptumo žyma ir atitinkamais atvejais iki TRES SECRET UE/ES TOP SECRET lygio slaptumo žyma pažymėta ESĮI. Prieš paskyrimą VSP arba VSP pavaduotojas gauna saugumo leidimą.

3. Komisijos atstovybės gali prašyti KSI leisti 1 ir 2 dalyse nustatytiems reikalavimams taikyti išimtį.

12 straipsnis

Saugiose zonose taikomos saugios eksploatacijos taisyklės

1. Atitinkamo Komisijos padalinio VSP kiekvienai saugiai zonai, už kurią jis atsako, parengia SecOPs.

2. VSP užtikrina, kad SecOPs apimtų šiuos reikalavimus:

a) darbo valandomis į saugią zoną patekti nelydimiems leidžiama tik tiems darbuotojams, kurie turi galiojantį saugumo leidimą ir kuriems, kaip nustatyta, būtina susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėtais dokumentais;

b) galimybė į saugią zoną patekti nelydimiems ne darbo valandomis suteikiama tik padalinio VSP, saugios zonos RKP, jų pavaduotojams ir Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato įgaliotiems darbuotojams;

c) įrašymo ir ryšių prietaisų, kaip antai mobiliųjų telefonų, kompiuterių, fotoaparatų ar kitų išmaniųjų prietaisų, saugiose zonose be išankstinio KSI leidimo naudoti neleidžiama; dėl bet kokios nukrypti leidžiančios nuostatos į KSI reikia kreiptis iš anksto; VSP veikia kaip kontaktinis asmuo;

d) visus vidaus ar išorės darbuotojus, kuriems reikia patekti į saugią zoną, bet kurie neatitinka a punkte nustatytų kriterijų, visada lydi ir prižiūri tinkamą leidimą turintis darbuotojas; bet koks toks patekimas į saugią zoną fiksuojamas prie įėjimo į saugią zoną laikomame registracijos žurnale;

e) VSP užtikrina, kad saugią zoną stebinčios įsibrovimo aptikimo sistemos būtų visada įjungtos ir tinkamai veiktų, ir rūpinasi visais susijusiais slaptažodžiais, raktais, PIN kodais arba kitais prieigos ir tapatybės nustatymo mechanizmais.

f) saugioje zonoje suveikus signalizacijai, apie tai pranešama Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratui, kuris nedelsdamas apie tai informuoja VSP;

g) suveikus signalizacijai ar įvykus saugumo incidentui, padalinio, kuriame yra saugi zona, VSP registruoja kiekvieną intervenciją;

h) turi būti nustatytos procedūros, taikomos saugioje zonoje suveikus signalizacijai arba susidarius ekstremaliajai padėčiai, įskaitant, jei reikia, darbuotojų evakavimą ir KSI vadovaujamos ekstremaliųjų padėčių grupės ir išorės skubiosios pagalbos tarnybų greito reagavimo užtikrinimą;

i) VSP nedelsdamas praneša KSI apie bet kokį saugumo pažeidimą, padarytą saugioje zonoje arba su ja susijusį, kad būtų nuspręsta, kaip tinkamai reaguoti;

j) be priežiūros paliekami atskiri saugios zonos kabinetai, salės ir seifai yra visada užrakinami;

k) darbuotojai negali įslaptintos informacijos aptarinėti saugios zonos koridoriuose ar kitose bendrojo naudojimo patalpose, kai netoliese esama leidimo neturinčių asmenų.

13 straipsnis

Saugumui užtikrinti naudojami raktai ir kodai

1. VSP tenka bendra atsakomybė už saugiose zonose ar patekti į jas naudojamų raktų ir kodų deramą priežiūrą ir saugojimą. Raktai ir kodai laikomi apsauginėje talpykloje ir saugomi bent tokiu pat lygiu kaip ir medžiaga, su kuria susipažinti jie suteikia galimybę.

2. VSP tvarko apsauginių talpyklų ir saugyklų registrą, taip pat atnaujinamą visų darbuotojų, kurie nelydimi gali jomis naudotis, sąrašą.

3. VSP tvarko apsauginių talpyklų ir saugyklų raktų, įskaitant darbuotojus, kuriems jie išduoti, registrą. Saugomas kiekvieno išduoto rakto kvitas, kuriame nurodomas rakto identifikavimo numeris, gavėjas, data ir laikas.

4. Raktai ir kodai išduodami tik tiems darbuotojams, kuriems „būtina žinoti“ ir kuriems suteiktas atitinkamas leidimas susipažinti su ESĮI. Kai tos sąlygos nebetenkinamos, VSP pareikalauja raktą grąžinti.

5. VSP atsarginius raktus ir visų kodų sąrašą saugo atskiruose užantspauduotuose, nepermatomuose, pasirašytuose vokuose su nurodyta data, kuriuos turi parūpinti už raktus atsakingas darbuotojas. Tie vokai laikomi apsauginėje talpykloje, priskirtoje aukščiausio slaptumo žymos lygio medžiagai, laikomai atitinkamoje talpykloje arba saugykloje.

6. Jei keičiant kodą arba raktą aptinkama voko suklastojimo ar sugadinimo žymių, VSP tai laiko saugumo incidentu ir nedelsdamas apie tai praneša KSI.

7. Apsauginių talpyklų kodų nustatymai saugiose zonose keičiami prižiūrint VSP. Kodai iš naujo nustatomi ne rečiau kaip kas 12 mėnesių ir visais atvejais:

a) gavus naują talpyklą arba įrengus naują užraktą (visų pirma nedelsiant keičiami numatytieji kodai);

b) neteisėtai atskleidus kodus arba įtarus jų neteisėtą atskleidimą;

c) asmeniui, kuriam išduotas kodas, prieigos nebereikia.

8. VSP registruoja 7 dalyje nurodytų kodų pakeitimų datas.

14 straipsnis

ESĮI evakuacijos ir sunaikinimo ekstremaliosios padėties atveju planai

1. Remdamasis Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato pateiktomis gairėmis, VSP padalinio vadovui padeda parengti ESĮI evakuacijos ir sunaikinimo ekstremaliosios padėties atveju planus.

2. VSP užtikrina, kad bet kokia įranga, reikalinga 1 dalyje numatytiems planams vykdyti, būtų lengvai prieinama ir geros eksploatacinės būklės.

3. VSP kartu su pareigūnais, paskirtais 1 dalyje numatytuose planuose, ne rečiau kaip kas 12 mėnesių peržiūri planų parengties būklę ir imasi visų jiems atnaujinti būtinų veiksmų.

15 straipsnis

Saugumo leidimai

1. VSP registruoja visas padalinio pareigas, kurioms užimti reikalingas Komisijos saugumo leidimas, ir tas pareigas užimančius darbuotojus. Reikalavimas gauti saugumo leidimą turi būti nurodytas įdarbinimo proceso metu pranešime apie laisvą darbo vietą ir apie jį kandidatui turi būti pranešta per pokalbį.

2. VSP prižiūri visus prašymus išduoti saugumo leidimus susipažinti su ESĮI. VSP yra kontaktinis asmuo padalinyje ir palaiko ryšius su KSI saugumo leidimų klausimais.

3. VSP pateikia prašymą pradėti saugumo leidimo išdavimo atitinkamam darbuotojui procedūrą ir užtikrina, kad darbuotojas nedelsdamas KSI grąžintų užpildytą nacionalinio asmens patikimumo pažymėjimo klausimyną.

4. VSP užtikrina, kad padalinio darbuotojai, kurių patikimumas patikrintas, sudalyvautų saugumo leidimui gauti privalomame ESĮI informaciniame susitikime.

5. Kad gautų informaciją apie visus pasikeitimus, susijusius su pareigų, kurioms užimti reikalingas saugumo leidimas, VSP reguliariai palaiko ryšius su padalinio žmogiškųjų išteklių tarnyba ir apie bet kokį tokį pakeitimą nedelsdamas informuoja KSI.

6. VSP informuoja KSI apie naujo darbuotojo, turinčio galiojantį asmens patikimumo pažymėjimą, kad galėtų užimti pareigas, kurias eiti gali saugumo leidimą turintis darbuotojas, atvykimą.

7. VSP užtikrina, kad padalinio darbuotojai iki nustatyto termino užbaigtų asmens patikimumo pažymėjimo atnaujinimo procedūrą. Bet kuris darbuotojas, kuris atsisako užbaigti procedūrą, privalo būti perkeltas į pareigas, kurias eiti gali saugumo leidimo neturintis darbuotojas.

16 straipsnis

ESĮI registratūra

1. Jei padalinyje veikia ESĮI registratūra, VSP prižiūri RKP veiklą, susijusią su ESĮI tvarkymu ir ESĮI apsaugai užtikrinti skirtų saugumo taisyklių laikymusi.

2. VSP ne rečiau kaip kas 12 mėnesių ir pasikeitus RKP arba RKP pavaduotojui atlieka šias patikras:

a) dokumentų imties ESĮI registratūroje patikrą, siekiant patvirtinti jų statusą ir įslaptintų dokumentų registro tikslumą;

b) į ESĮI registratūrą atsiųstos ir iš jos išsiųstos ESĮI gavimą ir išsiuntimą patvirtinančių kvitų imties patikrą;

c) sunaikinimo aktų imties patikrą.

3. Kad įsitikintų, jog dokumentai yra teisingai registruojami, VSP bent kartą per mėnesį vietoje atlieka įslaptintų dokumentų registro ir neseniai gautų įslaptintų dokumentų patikras.

4. Visos patikros registruojamos įslaptintų dokumentų registro žurnale.

17 straipsnis

Kita su saugumu susijusi atsakomybė

Kita su saugumu susijusi atsakomybė, tenkanti VSP, nustatoma saugumo pranešime, kuriame visų pirma nurodomas fizinis asmenų, patalpų ir kito turto bei informacijos saugumas.

5 SKYRIUS

Registracijos kontrolės pareigūnas

18 straipsnis

RKP paskyrimas

1. RKP ir RKP pavaduotojai yra pareigūnai arba laikinieji darbuotojai.

2. Visi RKP ir RKP pavaduotojai turi turėti galiojantį saugumo leidimą susipažinti su iki SECRET UE/ES SECRET lygio slaptumo žyma ir atitinkamais atvejais iki TRES SECRET UE/ES TOP SECRET lygio slaptumo žyma pažymėta ESĮI. Prieš paskyrimą RKP arba RKP pavaduotojas gauna saugumo leidimą.

3. Komisijos atstovybės gali prašyti KSI leisti 1 ir 2 dalyse nustatytiems reikalavimams taikyti išimtį.

19 straipsnis

Atsakomybė

1. RKP saugumo sumetimais registruoja CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėtą informaciją, kai:

a) ji pasiekia Komisijos padalinį ar iš jo išsiunčiama arba

b) ji pasiekia RIS ar iš jos išsiunčiama.

2. RKP registruoja visus įvykius per visą CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėtos informacijos gyvavimo ciklą. RKP taip pat užtikrina, kad būtų registruojama visa RESTREINT UE/ES RESTRICTED arba lygiaverčio lygio slaptumo žyma pažymėta informacija, kuria keičiamasi su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis. Tai atliekama derinant veiksmus su Generalinio sekretoriato administruojama ESĮI registratūra.

3. RKP registruoja CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėtus dokumentus įslaptintų dokumentų registre ir užtikrina, kad jie būtų saugiai laikomi ESĮI registratūroje.

4. RKP Komisijos darbuotojams padeda rengti ir siųsti CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėtą informaciją.

5. Kai CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėti dokumentai gaunami iš kitų padalinių ar išorės šalių, RKP užtikrina, kad rengėjui būtų tinkamai grąžinta pristatymo patvirtinimo forma.

6. Prieš leisdamas darbuotojui susipažinti su ESĮI registratūroje saugomu įslaptintu dokumentu, RKP kartu su VSP patikrina, ar darbuotojas yra gavęs KSI saugumo leidimą.

7. RKP registruoja visus į ESĮI registratūrą įeinančius ir iš jos išeinančius darbuotojus, kuriems nesuteiktas leidimas nelydimiems su tokiais dokumentais susipažinti, ir juos lydi vizito metu.

8. Kai darbuotojas, norėdamas susipažinti su dokumentu, jį iš ESĮI registratūros išsineša, RKP užtikrina, kad darbuotojas būtų susipažinęs su atitinkamomis kompensacinėmis saugumo priemonėmis ir kad dokumentą, kai tik jo nebereikia, grąžintų. RKP darbuotojams primena visus tokius dokumentus kuo greičiau grąžinti.

9. Jei įslaptinti dokumentai gabenami už valstybės, kurioje yra registratūra, ribų, ESĮI registratūra išduoda kurjerio pažymėjimą.

10. Išsamios RKP instrukcijos dėl įslaptintų dokumentų registravimo pateikiamos saugumo pranešime.

20 straipsnis

Slaptumo lygio sumažinimas ir išslaptinimas

RKP padeda dokumentus rengiantiems padaliniams peržiūrėti registruotą ESĮI, siekiant nustatyti, ar pirminis slaptumo žymos lygis vis dar tinkamas arba ar dokumento slaptumo lygis gali būti sumažintas, ar dokumentas gali būti išslaptintas.

21 straipsnis

Sunaikinimas

1. RKP atsako už CONFIDENTIEL UE/ES CONFIDENTIAL ir aukštesnio lygio slaptumo žyma pažymėtos informacijos sunaikinimą patvirtintomis priemonėmis, prireikus dalyvaujant liudytojams, kurių patikimumas patikrintas.

2. Bet kokios CONFIDENTIEL UE/ES CONFIDENTIAL ir aukštesnio lygio slaptumo žyma pažymėtos informacijos sunaikinimą RKP registruoja įslaptintų dokumentų registre, o atitinkamus sunaikinimo aktus saugo ESĮI registratūroje.

22 straipsnis

Papildomos užduotys

1. VSP vykdant priežiūros veiklą ESĮI registratūroje, RKP teikia VSP visą būtiną pagalbą.

2. RKP praneša VSP apie visus įtariamus ar faktinius saugumo incidentus, o VSP savo ruožtu apie juos praneša KSI.

3. Kai Komisijos padalinys rengia susitikimą, kuriame bus naudojama CONFIDENTIEL UE/ES CONFIDENTIAL ar aukštesnio lygio slaptumo žyma pažymėta informacija, to padalinio ESĮI registratūros RKP parengia ESĮI, kuri bus aptarta susitikime, ir su susitikimo rengėju koordinuoja veiklą, kad užtikrintų, jog visi dokumentai ir kvitai būtų tvarkomi laikantis atitinkamų taisyklių.

6 SKYRIUS

Baigiamosios nuostatos

23 straipsnis

Skaidrumas

Apie šį sprendimą informuojami Komisijos darbuotojai ir visi asmenys, kuriems jis taikomas, ir jis paskelbiamas *Europos Sąjungos oficialiajame leidinyje*.

24 straipsnis

Šis sprendimas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Priimta Briuselyje 2022 m. balandžio 7 d.

Komisijos vardu
Pirmininkės pavedimu
Gertrud INGESTAD
Generalinė direktorė
Žmogiškųjų išteklių ir saugumo generalinis direktoratas