EUROOPA
KOMISJON

Brüssel, 23.6.2020
COM(2020) 255 final

ANNEX

LISA

järgmise dokumendi juurde:

Ettepanek: Nõukogu otsus

seisukoha kohta, mis võetakse Euroopa Liidu nimel Euroopa Liidu ja Šveitsi Konföderatsiooni vahelise kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepinguga asutatud ühiskomitees seoses ühiste töömenetluste vastuvõtmisega

EUROOPA LIIDU JA ŠVEITSI KONFÖDERATSIOONI VAHELISE KASVUHOONEGAASIDE HEITKOGUSTEGA KAUPLEMISE SÜSTEEMIDE SIDUMISE LEPINGUGA ASUTATUD ÜHISKOMITEE OTSUS nr 1/2020,

...,

ühiste töömenetluste kohta

ÜHISKOMITEE,

võttes arvesse Euroopa Liidu ja Šveitsi Konföderatsiooni vahelist kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepingut[1], (edaspidi „leping“), eriti selle artiklit 3,

ning arvestades järgmist:

(1) Ühiskomitee 5. detsembri 2019. aasta otsusega nr 2/2019 muudeti lepingu I ja II lisa, millega täideti lepingus sätestatud sidumise tingimused.

(2) Pärast ühiskomitee otsuse nr 2/2019 vastuvõtmist ja vastavalt lepingu artikli 21 lõikele 3 vahetasid lepinguosalised oma ratifitseerimis- või heakskiitmiskirju, kuna nad loevad kõiki lepingus sätestatud sidumise tingimusi täidetuks.

(3) Kooskõlas lepingu artikli 21 lõikega 4 jõustus leping 1. jaanuaril 2020.

(4) Lepingu artikli 3 lõike 6 kohaselt peaksid Šveitsi registri haldaja ja liidu registri põhihaldaja (lepingus „keskregistrihaldaja“) koostama ühised töömenetlused (lepingus „ühine tegevuskord“), mis on seotud liidu registri Euroopa Liidu tehingulogi ja Šveitsi registri Šveitsi täiendava tehingulogi vahelise ühenduse toimimiseks vajalike tehniliste ja muude aspektidega, võttes arvesse riigisisestes õigusaktides sätestatud prioriteete. Ühised töömenetlused peaksid jõustuma ühiskomitee otsuse alusel.

(5) Kooskõlas artikli 13 lõikega 1 peaks ühiskomitee leppima kokku tehnilistes suunistes, et tagada lepingu nõuetekohane rakendamine, sealhulgas tehnilistes või muudes aspektides, mis on vajalikud ühenduse toimimiseks, võttes arvesse riigisisestes õigusaktides sätestatud prioriteete. Tehnilised suunised võib välja töötada lepingu artikli 12 lõike 5 kohaselt moodustatud töörühm. Töörühma peaksid kuuluma vähemalt Šveitsi registri haldaja ja liidu registri põhihaldaja ning töörühm peaks abistama ühiskomiteed lepingu artikli 13 kohaste ülesannete täitmisel.

(6) Arvestades suuniste tehnilist laadi ja vajadust kohandada neid toimuva arenguga, tuleks Šveitsi registri haldaja ja liidu põhihaldaja välja töötatud tehnilised suunised esitada ühiskomiteele teadmiseks või vajaduse korral heakskiitmiseks,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Võetakse vastu käesolevale otsusele lisatud ühised töömenetlused.

Artikkel 2

Käesolevaga moodustatakse töörühm vastavalt lepingu artikli 12 lõikele 5. Töörühm abistab ühiskomiteed, et tagada lepingu nõuetekohane rakendamine, sealhulgas ühiste töömenetluste rakendamiseks vajalike tehniliste suuniste väljatöötamine.

[1] ELT L 322, 7.12.2017, lk 3.

Töörühma kuuluvad vähemalt Šveitsi registri haldaja ja liidu registri põhihaldaja.

Artikkel 3

Käesolev otsus jõustub selle vastuvõtmise päeval.

Koostatud inglise keeles Brüsselis, XX 2020.

Ühiskomitee nimel

Euroopa Liidu määratud sekretär	*eesistuja*	*Šveitsi määratud sekretär*

LIIDE

LISA

ÜHISED TÖÖMENETLUSED

vastavalt Euroopa Liidu ja Šveitsi Konföderatsiooni vahelise kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepingu artikli 3 lõikele 6
- Menetlused ajutise lahenduse jaoks -

1. MÕISTED

Tabel 1-1 Akronüümid ja mõisted

Akronüüm/termin	Mõiste
Sertifitseerimisasutus	Elektroonilisi sertifikaate väljastav üksus
Šveits	Šveitsi Konföderatsioon
HKS	Heitkogustega kauplemise süsteem
EL	Euroopa Liit
IHR	Intsidendihaldusrühm
Teabevara	Teave, mis on ettevõttele või organisatsioonile väärtuslik
IT	Infotehnoloogia
ITIL	Infotehnoloogia infrastruktuuri andmik (*Information Technology Infrastructure Library)*
ITTH	IT-teenuste haldus
ÜTS	Ühenduse tehniline standard
Register	HKSi raames välja antud lubatud heitkoguse ühikute (LHÜd) arvestussüsteem, mille abil jälgitakse, kellele kuuluvad elektroonilistel kontodel hoitavad LHÜd.
MT	Muudatuse taotlus
TTL	Tundliku teabe loetelu
TS	Teenindussoov
Viki	Veebisait, mille abil kasutajad saavad vahetada teavet ja teadmisi sisu lisamise või kohandamisega otse veebilehitseja kaudu.

2. SISSEJUHATUS

Euroopa Liidu ja Šveitsi Konföderatsiooni vahel 23. novembril 2017 sõlmitud kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepinguga (edaspidi „leping“) nähakse ette selliste lubatud heitkoguse ühikute (edaspidi „LHÜd“) vastastikune tunnustamine, mida saab kasutada kohustuste täitmiseks Euroopa Liidu heitkogustega kauplemise süsteemis (edaspidi „ELi HKS“) või Šveitsi heitkogustega kauplemise süsteemis (edaspidi „Šveitsi HKS“). ELi HKSi ja Šveitsi HKSi vahelise ühenduse töölerakendamiseks tuleb luua otseside liidu registri ELi tehingulogi ja Šveitsi registri täiendava tehingulogi vahel, mis võimaldab kummaski HKSis välja antud LHÜde ülekandmist ühest registrist teise (lepingu artikli 3 lõige 2). ELi HKSi ja Šveitsi HKSi vahelise ühenduse töölerakendamiseks võetakse 2020. aasta maiks või esimesel võimalusel kasutusele ajutine lahendus. Lepinguosalised teevad koostööd, et asendada ajutine registriühenduse lahendus alalisega niipea kui võimalik (lepingu II lisa).

Lepingu artikli 3 lõike 6 kohaselt peavad Šveitsi registri haldaja ja liidu registri põhihaldaja (lepingus „keskregistrihaldaja“) koostama ühised töömenetlused (lepingus „ühine tegevuskord“), mis on seotud ühenduse toimimiseks vajalike tehniliste ja muude aspektidega, võttes arvesse riigisisestes õigusaktides sätestatud prioriteete. Haldajate koostatud ühised töömenetlused jõustuvad ühiskomitee otsuse alusel.

Käesolevas dokumendis esitatud ühised töömenetlused on ühiskomiteel kavas vastu võtta otsusega nr 1/2020. Kooskõlas käesoleva otsusega palub ühiskomitee Šveitsi registri haldajal ja liidu põhihaldajal töötada välja edasised tehnilised suunised registritevahelise ühenduse töölerakendamiseks ning tagada nende pidev kohandamine tehnika arenguga ning ühenduse ohutuse ja turvalisuse ning selle tõhusa ja tulemusliku toimimisega seotud uute nõuetega.

2.1. Kohaldamisala

Käesolev dokument kujutab endast lepinguosaliste ühist arusaama ELi HKSi registri ja Šveitsi HKSi registri vahelise ühenduse menetluslike aluste loomisest. Selles kirjeldatakse ühenduse toimimisega seotud üldisi menetlusnõudeid, aga ühenduse töölerakendamiseks on vaja täiendavaid tehnilisi suuniseid.

Ühenduse nõuetekohaseks toimimiseks on vaja tehnilist kirjeldust, et ühenduse töölerakendamisega edasi liikuda. Lepingu artikli 3 lõike 7 kohaselt käsitletakse neid küsimusi üksikasjalikult ühenduse tehnilises standardis, mille ühiskomitee eraldi otsusega vastu võtab.

Ühiste töömenetluste eesmärk on tagada, et ELi HKSi registri ja Šveitsi HKSi registri vahelise ühenduse toimimisega seotud IT-teenuseid osutatakse tulemuslikult ja tõhusalt, eelkõige teenindussoovide täitmiseks, teenusetõrgete kõrvaldamiseks, probleemide lahendamiseks ning rutiinsete operatiivülesannete täitmiseks vastavalt IT-teenuste halduse rahvusvahelistele standarditele.

Kokkulepitud ajutise lahenduse jaoks on vaja üksnes järgmisi ühiseid töömenetlusi, mis on esitatud käesolevas dokumendis:

- intsidendihaldus;
- probleemihaldus;
- teenindussoovi täitmine;
- muudatusehaldus;
- väljalaskehaldus;

- turvaintsidendi haldus;
- infoturbe haldus.

Hiljem alalise registriühenduse juurutamisel tuleb ühiseid töömenetlusi kohandada ja vajaduse korral täiendada.

2.2. Adressaadid

Ühised töömenetlused on mõeldud ELi ja Šveitsi registri tugirühmadele.

3. LÄHENEMISVIIS JA STANDARDID

Kõigi ühiste töömenetluste suhtes kohaldatakse järgmist põhimõtet:

- EL ja Šveits lepivad kokku, et ühised töömenetlused määratakse kindlaks ITILi (infotehnoloogia infrastruktuuri andmik, versioon 3) alusel. Selle standardi kohaseid tavasid taaskasutatakse ja neid kohandatakse ajutise lahendusega seotud erivajadustele.
- Ühiste töömenetluste rakendamiseks vajalik teabevahetus ja koordineerimine toimub Šveitsi ja ELi registrite kasutajatugede kaudu. Ülesanded määratakse alati ühe lepinguosalise siseselt.
- Kui ühise töömenetluse suhtes tekib lahkarvamusi, analüüsitakse seda ja lahendatakse see mõlema kasutajatoe koostöös. Kui kokkuleppele ei jõuta, eskaleeritakse ühise lahenduse leidmine järgmisele tasemele.

Eskalatsioonitasemed	**EL**	**Šveits**
1. tase	ELi kasutajatugi	Šveitsi kasutajatugi
2. tase	ELi käitusjuht	Šveitsi registri rakendusjuht
3. tase	Ühiskomitee (kes võib lepingu artikli 12 lõiget 5 arvesse võttes selle ülesande delegeerida)	
4. tase	Ühiskomitee, kui 3. tase delegeeritakse	

- Kumbki lepinguosaline võib määrata kindlaks oma registrisüsteemi toimimise korra, võttes arvesse käesolevate ühiste töömenetlustega seotud nõudeid ja liideseid.
- Ühiste töömenetluste, eelkõige intsidendihalduse, probleemihalduse ja teenindussoovide täitmise, ning lepinguosaliste vahelise suhtluse toetamiseks kasutatakse IT-teenuste haldusvahendit.
- Lisaks on lubatud teabevahetus e-posti teel.
- Mõlemad lepinguosalised tagavad, et infoturbenõudeid täidetakse vastavalt käitlemisjuhistele.

4. INTSIDENDIHALDUS

Intsidendihaldusprotsessi eesmärk on taastada IT-teenuste tavapärane teenustase võimalikult kiiresti ja selliselt, et äritegevuse katkestus oleks minimaalne.

Intsidendihalduse raames tuleks samuti pidada intsidentide registrit aruandluse jaoks ja seda tuleks lõimida muude protsessidega, et soodustada pidevat täiustamist.

- Intsidendihaldus hõlmab üldjoontes järgmisi tegevusi:
- intsidendi tuvastamine ja registreerimine;
- klassifitseerimine ja esmane tugi;
- uurimine ja diagnoosimine;
- lahendamine ja teenuse taastamine;
- intsidendi sulgemine.

Intsidendi kogu elutsükli jooksul vastutab intsidendihaldusprotsess pidevalt intsidendiga tegelejate määramise, intsidendi seire, jälgimise ja intsidendiga seotud teabevahetuse korraldamise eest.

4.1. Intsidentide tuvastamine ja registreerimine

Intsidendi võib tuvastada tugirühm, automaatsed seirevahendid või rutiinset järelevalvet teostav tehniline personal.

Kui intsident on tuvastatud, tuleb see registreerida ja sellele tuleb määrata kordumatu tunnuskood, mis võimaldab intsidenti nõuetekohaselt jälgida ja seirata. Intsidendi kordumatu tunnuskood on identifikaator, mille ühises piletisüsteemis määrab intsidendi tõstatanud lepinguosalise (ELi või Šveitsi) kasutajatugi, ning seda tuleb kasutada selle intsidendiga seotud kogu teabevahetuses.

Kõigi intsidentide puhul peaks kontaktpunkt olema pileti registreerinud lepinguosalise kasutajatugi.

4.2. Klassifitseerimine ja esmane tugi

Intsidentide klassifitseerimise eesmärk on mõista ja kindlaks teha, milline süsteem ja/või teenus on mõjutatud ja mil määral. Selleks et klassifitseerimine oleks tõhus, peaks see suunama intsidendi esimese katsega õige ressursi juurde, et kiirendada intsidendi lahendamist.

Klassifitseerimisetapis tuleks intsident liigitada ja prioriseerida vastavalt selle mõjule ja kiireloomulisusele, et seda saaks käsitleda vastavalt prioriteetsusest sõltuvale ajakavale.

Kui intsident võib mõjutada tundlike andmete konfidentsiaalsust või terviklust ja/või mõjutab süsteemi käideldavust, loetakse intsident ka turvaintsidendiks ja seda käsitletakse vastavalt käesoleva dokumendi peatükis „Turvaintsidentide haldus“ kirjeldatud protsessile.

Võimaluse korral teostab pileti registreerinud kasutajatugi esmase diagnoosimise. Selleks kontrollib kasutajatugi, kas intsident on teadaolev viga. Kui see on nii, siis on lahendustee või hädalahendus juba teada ja dokumenteeritud.

Kui kasutajatugi suudab intsidendi edukalt lahendada, sulgeb ta intsidendi selles etapis, kuna intsidendihalduse peamine eesmärk (st lõppkasutaja jaoks teenuse kiire taastamine) on täidetud. Kui see nii ei ole, eskaleerib kasutajatugi juhtumi edasiseks uurimiseks ja diagnoosimiseks asjakohasele lahendajate rühmale.

4.3. Uurimine ja diagnoosimine

Intsidenti uuritakse ja diagnoositakse juhul, kui kasutajatugi ei suuda esialgse diagnoosimise käigus intsidenti lahendada ning see eskaleeritakse. Intsidendi eskaleerimine on uurimise ja diagnoosimise protsessi lahutamatu osa.

Uurimis- ja diagnoosimisetapis on tavapärane proovida intsidenti kontrollitud tingimustes uuesti esile kutsuda. Intsidendi uurimisel ja diagnoosimisel on oluline mõista intsidendini viinud sündmuste õiget järjekorda.

Eskaleerimine tähendab tõdemust, et intsidenti ei suudeta asjaomasel kasutajatoe tasandil lahendada ning see tuleb edastada kõrgema tasandi tugirühmale või teisele lepinguosalisele. Eskaleerimine võib toimuda kahel viisil: horisontaalselt (funktsionaalne) või vertikaalselt (hierarhiline).

Intsidendi registreerinud ja käivitanud kasutajatugi vastutab intsidendi eskaleerimise eest asjakohasele ressursile ning intsidendi üldise seisu ja sellega tegelejate määramise jälgimise eest.

Lepinguosaline, kellele intsident on määratud, vastutab taotletud tegevuste õigeaegse elluviimise ja oma kasutajatoele tagasiside andmise eest.

4.4. Lahendamine ja teenuse taastamine

Intsidendi lahendamine ja teenuse taastamine toimub siis, kui intsidendist on täielikult aru saadud. Intsidendile lahenduse leidmine tähendab, et on kindlaks tehtud viis vea parandamiseks. Lahenduse kohaldamine on teenuse taastamise etapp.

Kui asjakohane ressurss on teenusetõrke kõrvaldanud, suunatakse intsident tagasi asjaomasele intsidendi registreerinud kasutajatoele, kes küsib intsidendi algatajalt kinnitust, et viga on parandatud ja intsidendi võib sulgeda. Intsidendi käsitlemisel tehtud järeldused tuleb dokumenteerida edaspidiseks kasutamiseks.

IT-toe töötajad võivad teenuse ise taastada või anda lõppkasutajale juhised, mille järgi teenus taastada.

4.5. Intsidendi sulgemine

Sulgemine on intsidendihaldusprotsessi viimane etapp ja see toimub varsti pärast intsidendi lahendamist.

Sulgemisetapi tegevuste kontrollnimekirjas pööratakse erilist tähelepanu järgmisele:

- intsidendile algselt määratud kategooria kontrollimine;
- intsidendiga seotud kogu teabe nõuetekohane registreerimine;
- intsidendi nõuetekohane dokumenteerimine ja teadmusbaasi ajakohastamine;
- kõigi intsidendist otseselt või kaudselt mõjutatud huvirühmade teavitamine.

Intsident on ametlikult suletud pärast seda, kui kasutajatugi on intsidendi sulgemise etapi lõpule viinud ja teatanud sellest teisele lepinguosalisele.

Kui intsident on suletud, ei avata seda uuesti. Kui intsident kordub lühikese aja jooksul, ei avata algset intsidenti uuesti, vaid registreeritakse uus intsident.

Kui intsidenti jälgivad nii ELi kui ka Šveitsi kasutajatoed, vastutab lõpliku sulgemise eest pileti registreerinud kasutajatugi.

5. PROBLEEMIHALDUS

Seda menetlust tuleks järgida alati, kui tuvastatakse probleem, mis käivitab probleemihaldusprotsessi. Probleemihalduses keskendutakse kvaliteedi parandamisele ja intsidentide arvu vähendamisele. Probleem võib olla ühe või mitme intsidendi põhjus. Kui teatatakse intsidendist, on intsidendihalduse eesmärk taastada teenus võimalikult kiiresti. See

võib hõlmata hädalahenduste kasutamist. Probleemi registreerimise korral on eesmärk uurida probleemi algpõhjust, et teha kindlaks muudatus, mis tagab, et probleemi ja sellega seotud intsidente enam ei esine.

5.1. Probleemi tuvastamine ja registreerimine

Sõltuvalt sellest, kumb lepinguosaline pileti lõi, on probleemidega seotud küsimustes kontaktpunktiks kas ELi või Šveitsi kasutajatugi.

Probleemi kordumatu tunnuskood on IT-teenuse haldusvahendi määratud identifikaator. Seda tuleb kasutada selle probleemiga seotud kogu teabevahetuses.

Probleemi registreerimiseks võib anda tõuke intsident või seda võidakse teha omaalgatuslikult, et lahendada süsteemis mis tahes etapis avastatud probleemid.

5.2. Probleemi prioriseerimine

Probleeme võib nende jälgimise lihtsustamiseks liigitada vastavalt nende raskusastmele ja tähtsusele samamoodi nagu intsidente, võttes arvesse nendega seotud intsidentide mõju ja esinemise sagedust.

5.3. Probleemi uurimine ja diagnoosimine

Probleemi võib tõstatada kumbki lepinguosaline ning algatava lepinguosalise kasutajatugi vastutab selle registreerimise, asjakohasele ressursile määramise ja selle üldise seisu jälgimise eest.

Lahendajate rühm, kellele probleem eskaleeriti, vastutab probleemi õigeaegse lahendamise ja kasutajatoega suhtlemise eest.

Taotluse korral vastutavad mõlemad lepinguosalised määratud ülesannete täitmise tagamise ja oma kasutajatoele tagasiside andmise eest.

5.4. Lahendamine

Lahendajate rühm, kellele probleem on määratud, vastutab selle lahendamise ja oma kasutajatoele asjakohase teabe esitamise eest.

Probleemi käsitlemisel tehtud järeldused tuleb dokumenteerida edaspidiseks kasutamiseks.

5.5. Probleemi sulgemine

Probleem on ametlikult suletud siis, kui see on muudatuse teostamisega lahendatud. Probleemi sulgemise etapi teostab see kasutajatugi, kes probleemi registreeris ja teise lepinguosalise kasutajatuge teavitas.

6. TEENINDUSSOOVI TÄITMINE

Teenindussoovi täitmise protsess on uue või olemasoleva teenuse taotluse täielik haldamine alates selle registreerimisest ja heakskiitmisest kuni sulgemiseni. Teenindussoovid on tavaliselt väikesed, eelnevalt määratletud, korratavad, sagedased, eelnevalt heaks kiidetud ja menetluslikud taotlused.

Allpool on kirjeldatud põhietappe, mida tuleb järgida.

6.1. Teenindussoovi algatamine

Teenindussooviga seotud teave esitatakse ELi või Šveitsi kasutajatoele e-posti, telefoni või IT-teenuse haldusvahendi või mis tahes muu kokkulepitud sidekanali kaudu.

6.2. Teenindussoovi registreerimine ja analüüsimine

Kõigi teenindussoovide puhul peaks kontaktpunkt olema ELi või Šveitsi kasutajatugi, olenevalt sellest, milline lepinguosaline teenindussoovi esitas. Selle kasutajatoe ülesanne on teenindussoov registreerida ja seda hoolikalt analüüsida.

6.3. Teenindussoovi heakskiitmine

Teenindussoovi esitanud lepinguosalise kasutajatoe spetsialist kontrollib, kas on vaja teise lepinguosalise heakskiitu, ja vajaduse korral hangib selle. Kui teenindussoovi heaks ei kiideta, ajakohastab kasutajatugi piletit ja sulgeb selle.

6.4. Teenindussoovi täitmine

Selle etapiga tagatakse teenindussoovi tulemuslik ja tõhus käsitlemine. Eristada tuleb kahte järgmist juhtu:

- teenindussoovi täitmine puudutab ainult ühte lepinguosalist. Sellisel juhul annab kõnealune lepinguosaline välja töökäsud ja koordineerib nende täitmist;
- teenindussoovi täitmine puudutab nii ELi kui ka Šveitsi. Sellisel juhul annavad kasutajatoed töökäsud oma vastutusalas. Kasutajatoed koordineerivad teenindussoovi täitmist omavahel. Üldine vastutus lasub teenindussoovi vastu võtnud ja algatanud kasutajatoel.

Kui teenindussoov on täidetud, tuleb selle seisuks määrata „täidetud“.

6.5. Teenindussoovi eskaleerimine

Vajaduse korral saab kasutajatugi eskaleerida täitmata teenindussoovid asjakohasele ressursile (kolmandale isikule).

Eskaleeritakse vastavatele kolmandatele isikutele, st ELi kasutajatugi peab Šveitsi kolmandale isikule eskaleerimiseks võtma ühendust Šveitsi kasutajatoega ja vastupidi.

Kolmas isik, kellele teenindussoov eskaleeriti, vastutab teenindussoovi õigeaegse täitmise ja selle eskaleerinud kasutajatoega suhtlemise eest.

Teenindussoovi registreerinud kasutajatugi vastutab teenindussoovi üldise seisu ja sellega tegelejate määramise jälgimise eest.

6.6. Teenindussoovi täitmise läbivaatamine

Vastutav kasutajatugi esitab teenindussoovi kirje lõplikuks kvaliteedikontrolliks enne selle sulgemist. Eesmärk on tagada, et teenindussoovi on tõepoolest käsitletud ja et teenindussoovi elutsükli kirjeldamiseks vajalik teave on esitatud piisavalt üksikasjalikult. Lisaks tuleb teenindussoovi käsitlemisel tehtud järeldused dokumenteerida edaspidiseks kasutamiseks.

6.7. Teenindussoovi sulgemine

Kui teenindussoovi täitma määratud osalejad nõustuvad, et teenindussoov on täidetud, ja teenindussoovi esitaja leiab, et juhtum on lahendatud, määratakse järgmiseks seisuks „suletud“.

Teenindussoov on ametlikult suletud pärast seda, kui teenindussoovi registreerinud kasutajatugi on teenindussoovi sulgemise etapi lõpule viinud ja teatanud sellest teisele lepinguosalisele.

7. MUUDATUSEHALDUS

Eesmärk on tagada, et IT-taristu kontrollimiseks kasutatakse kõigi muudatuste tõhusaks ja kiireks käsitlemiseks standardmeetodeid ja -menetlusi, et minimeerida mis tahes seotud intsidentide arvu ja nende mõju teenusele. Muudatused IT-taristus võidakse teha probleemide lahendamise või väljastpoolt kehtestatud nõuete (nt muudetud õigusnormid) tulemusena või ennetavalt, püüdes suurendada tõhusust ja tulemuslikkust, või et võimaldada või kajastada ärialgatusi.

Muudatusehalduse protsess hõlmab eri etappe, mis registreerivad muudatuse taotluse iga üksikasja edasiseks jälgimiseks. Need protsessid tagavad, et muudatus valideeritakse ja seda testitakse enne selle juurutamist. Muudatusehalduse protsess vastutab eduka juurutamise eest.

7.1. Muudatuse taotlus

Muudatuse taotlus esitatakse muudatusehalduse rühmale valideerimiseks ja heakskiitmiseks. Kõigi muudatuse taotluste puhul peaks kontaktpunkt olema ELi või Šveitsi kasutajatugi, olenevalt sellest, milline lepinguosaline muudatuse taotluse esitas. Selle kasutajatoe ülesanne on muudatuse taotlus registreerida ja seda hoolikalt analüüsida.

Muudatuse taotlused võivad pärineda

- muutust põhjustavast intsidendist;
- olemasolevast probleemist, mis toob kaasa muudatuse;
- lõppkasutajalt, kes taotleb uut muudatust;
- käimasolevast hooldusest tulenevast muudatusest;
- õigusnormide muudatustest.

7.2. Muudatuse hindamine ja planeerimine

Selles etapis käsitletakse muudatuse hindamist ja planeerimist. See hõlmab prioriteetide seadmist ja planeerimist, et minimeerida riske ja mõju.

Kui taotletud muudatuse teostamine mõjutab nii ELi kui ka Šveitsi, kontrollib muudatuse taotluse registreerinud lepinguosaline muudatuse hindamist ja planeerimist koos teise lepinguosalisega.

7.3. Muudatuse heakskiitmine

Iga registreeritud muudatuse taotlus tuleb heaks kiita asjaomasel eskalatsioonitasemel.

7.4. Muudatuse teostamine

Muudatus teostatakse väljalaskehalduses. Mõlema lepinguosalise väljalaskehalduse rühmad järgivad oma protsesse, mis hõlmavad planeerimist ja testimist. Muudatuse hindamine toimub pärast selle teostamist. Plaanipärase teostamise tagamiseks vaadatakse olemasolevat muudatusehalduse protsessi pidevalt läbi ja vajaduse korral seda ajakohastatakse.

8. VÄLJALASKEHALDUS

Väljalaskega tehakse IT-teenuses üks või mitu muudatust, mis koondatakse väljalaskekavasse ja mis tuleb koos heaks kiita, ette valmistada ja luua ning mida tuleb koos testida ja juurutada. Üks väljalase võib hõlmata veaparandust, muudatust riistvaras või muudes komponentides, tarkvaramuudatusi, rakenduse uut versiooni, muudatusi dokumentatsioonis ja/või protsessides. Iga väljalaske sisu hallatakse, testitakse ja juurutatakse ühe üksusena.

Väljalaskehalduse eesmärk on planeerida, luua, testida, valideerida ja tarnida võimet osutada kavandatud teenuseid, et täita huvirühmade nõuded ja saavutada seatud eesmärgid. Kõigi teenuses tehtavate muudatuste vastuvõtukriteeriumid määratakse kindlaks ja dokumenteeritakse kavandamise koordineerimise käigus ning need esitatakse väljalaskehalduse rühmadele.

Väljalase koosneb tavaliselt veaparandustest ja teenuse täiustustest. See sisaldab uut või muudetud tarkvara ja mis tahes uut või muudetud riistvara, mida on vaja heakskiidetud muudatuste teostamiseks.

8.1. Väljalaske planeerimine

Protsessi esimeses etapis jaotatakse loa saanud muudatused väljalaskepakettide vahel ning määratakse kindlaks väljalasete ulatus ja sisu. Selle teabe põhjal koostatakse väljalaske planeerimise alamprotsessis väljalaske loomise, testimise ja juurutamise graafik.

Planeerimisel tuleks määrata kindlaks:

- väljalaske ulatus ja sisu;
- väljalaske riskihinnang ja riskiprofiil;
- kliendid/kasutajad, keda väljalase mõjutab;
- väljalaske eest vastutav rühm;
- tarne- ja juurutamisstrateegia;
- väljalaske ja juurutamise jaoks vajalikud vahendid.

Mõlemad lepinguosalised teavitavad teineteist oma väljalaskeplaanist ja hooldusajast. Kui väljalase mõjutab nii ELi kui ka Šveitsi, koordineerivad nad planeerimist ja määravad ühise hooldusaja.

8.2. Väljalaskepaketi loomine ja testimine

Väljalaskehaldusprotsessi loomis- ja testimisetapis määratakse lähenemisviis väljalaske või väljalaskepaketi rakendamiseks ja kontrollitud keskkondade säilitamiseks enne toodangversiooni muutmist, samuti kõigi muudatuste testimiseks kõigis välja lastud keskkondades.

Kui väljalase mõjutab nii ELi kui ka Šveitsi, koordineerivad nad tarneplaane ja määravad ühise hooldusaja. See hõlmab järgmisi aspekte:

- kuidas ja millal väljalaskeüksused ja teenuse komponendid tarnitakse;
- millised on tüüpilised üleminekuajad; mis juhtub hilinemise korral;
- kuidas jälgida tarne edenemist ja saada kinnitus;
- parameetrid väljalaske juurutamisega seotud jõupingutuste edukuse jälgimiseks ja kindlakstegemiseks;
- ühised testjuhtumid asjakohaste funktsioonide ja muudatuste jaoks.

Selle alamprotsessi lõpuks on kõik nõutavad väljalaskekomponendid valmis liikuma tootmiskeskkonnas juurutamise etappi.

8.3. Juurutamise ettevalmistamine

Ettevalmistamise alamprotsessiga tagatakse, et teavituskavad on õigesti koostatud ja teated on valmis saatmiseks kõigile mõjutatud huvirühmadele ja lõppkasutajatele, ning et väljalase on

lõimitud muudatusehalduse protsessiga, tagamaks, et kõik muudatused tehakse kontrollitud viisil ja et neil on nõutud üksuste heakskiit.

Kui väljalase mõjutab nii ELi kui ka Šveitsi, koordineerivad nad järgmisi tegevusi:

- muudatuse taotluse registreerimine tootmiskeskkonnas juurutamise ajastamiseks ja ettevalmistamiseks;
- teostusplaani loomine;
- tagasipööramiskava, et juurutamise ebaõnnestumise korral saaks eelmise oleku taastada;
- kõigile vajalikele osalistele teadete saatmine;
- asjakohaselt eskalatsioonitasemelt väljalaske rakendamiseks heakskiidu saamine.

8.4. Väljalaske tagasipööramine

Kui juurutamine ebaõnnestub või kui testimise käigus tehakse kindlaks, et juurutamine ei olnud edukas või ei vastanud kokkulepitud vastuvõtu-/kvaliteedikriteeriumidele, peavad mõlema lepinguosalise väljalaskehalduse rühmad pöörduma tagasi eelmise oleku juurde. Teavitada tuleb kõiki vajalikke huvirühmi, sealhulgas mõjutatud või sihtrühmaks olevaid lõppkasutajaid. Kuni heakskiidu saamiseni saab protsessi uuesti alustada mis tahes eelnevas etapis.

8.5. Väljalaske hindamine ja sulgemine

Väljalaske hindamise käigus tuleks teha järgmist:

- koguda tagasisidet selle kohta, milline on klientide ja kasutajate rahulolu väljalaske juurutamise ja teenuse osutamisega (arvestada saadud tagasisidet teenuse pidevaks täiustamiseks);
- vaadata läbi kvaliteedikriteeriumid, mida ei täidetud;
- kontrollida, et kõik toimingud, vajalikud parandused ja muudatused on teostatud;
- veenduda, et pärast juurutamist ei ole mingeid võimekuse, ressursside, suutlikkuse või tulemuslikkusega seotud probleeme;
- kontrollida, et kõik probleemid, teadaolevad vead ja hädalahendused on dokumenteeritud ning kliendi, lõppkasutaja, operatiivtoe ja teiste mõjutatud poolte jaoks vastuvõetavad;
- jälgida väljalaskest põhjustatud intsidente ja probleeme (pakkuda operatiivrühmadele sissetöötamistuge, kui väljalase on suurendanud töömahtu);
- ajakohastada tugidokumente (st tehnilise teabe dokumente);
- anda väljalaske juurutamine ametlikult üle teenuse käitusele;
- dokumenteerida saadud õppetunnid;
- koguda rakendusrühmadelt väljalaske kokkuvõtte dokumendid;
- sulgeda väljalase ametlikult pärast muudatuse taotluse kirje kontrollimist.

9. TURVAINTSIDENDI HALDUS

Turvaintsidentide haldus kujutab endast turvaintsidentide käsitlemise protsessi, mis võimaldab intsidendist potentsiaalselt mõjutatud huvirühmi teavitada, intsidenti hinnata ja prioriseerida ning intsidendile reageerida, et lahendada tundlike teabevarade konfidentsiaalsuse, käideldavuse või terviklusega seotud tegelik, kahtlustatav või võimalik rikkumine.

9.1. Turvaintsidendi kategoriseerimine

Kõiki liidu registri ja Šveitsi registri vahelist seost mõjutavaid intsidente analüüsitakse, et teha kindlaks tundliku teabe loetellu kantud mis tahes tundliku teabe konfidentsiaalsuse, tervikluse või käideldavuse võimalik rikkumine.

Rikkumise korral kirjeldatakse intsidenti kui turvaintsidenti, mis registreeritakse viivitamata IT-teenuse haldusvahendis ja mida hallatakse sellisena.

9.2. Turvaintsidendi käsitlemine

Turvaintsidentide eest vastutab kolmas eskalatsioonitase ja intsidentide lahendamisega tegeleb spetsiaalne intsidendihaldusrühm (IHR).

IHRi ülesanded on järgmised:

- teha esimene analüüs, kategoriseerida ja hinnata intsidendi tõsidust;
- koordineerida kõigi huvirühmade tegevust, sealhulgas dokumenteerida täielikult intsidendi analüüs, intsidendi lahendamiseks tehtud otsused ja leitud võimalikud puudused;
- eskaleerida turvaintsident sõltuvalt selle tõsidusest aegsasti asjakohasele tasemele teabe saamiseks või otsuse tegemiseks.

Infoturbe haldamise protsessis klassifitseeritakse kogu intsidentidega seotud teave kõige kõrgemale tundlikkustasemele, kuid mitte madalamale kui „TUNDLIK HKS“.

Käimasoleva uurimise ja/või puuduse korral, mida võidakse ära kasutada, ja kuni selle parandamiseni määratakse teabe tundlikkustasemeks „KRIITILINE HKS“.

9.3. Turvaintsidendi identifitseerimine

Infoturbeametnik määrab turvasündmuse liigi põhjal kindlaks asjakohased organisatsioonid, kes kaasatakse ja kes hakkavad kuuluma IHRi.

9.4. Turvaintsidendi analüüs

IHR teeb vastavalt vajadusele koostööd kõigi kaasatud organisatsioonide ja nende vastavate rühmade asjaomaste liikmetega, et intsidenti hinnata. Analüüsi käigus tehakse kindlaks vara konfidentsiaalsuse, tervikluse või käideldavuse vähenemise ulatus ning hinnatakse tagajärgi kõigile mõjutatud organisatsioonidele. Seejärel määratakse kindlaks esialgsed ja järelmeetmed intsidendi lahendamiseks ja selle mõju ohjamiseks, sealhulgas nende meetmete mõju ressurssidele.

9.5. Turvaintsidendi tõsiduse hindamine, intsidendi eskaleerimine ja aruandlus

IHR hindab uute turvaintsidentide tõsidust pärast nende kirjeldamist ja alustab kohe nõuetekohast tegevust vastavalt intsidendi tõsidusele.

9.6. Turvaintsidendi lahenduse aruanne

IHR lisab turvaintsidendi lahendamise aruandesse intsidendi ohjeldamise ja sellest taastumise tulemused. Aruanne esitatakse kolmandale eskalatsioonitasemele turvatud e-kirja teel või muude mõlemapoolselt tunnustatud turvaliste sidevahendite abil.

Vastutav lepinguosaline vaatab intsidendi ohjeldamise ja sellest taastumise tulemused läbi ning

- taasühendab registri eelneva lahtiühendamise korral;
- annab registri meeskondadele intsidendi kohta teavet;
- sulgeb intsidendi.

IHR peaks turvalisel viisil lisama turvaintsidendi aruandesse asjakohased üksikasjad, et tagada järjepidev dokumenteerimine ja teabevahetus ning võimaldada kiireid ja sobivaid meetmeid intsidendi ohjeldamiseks. Pärast intsidendi lahendamist esitab IHR õigeaegselt turvaintsidendi lõpparuande.

9.7. Järelevalve, suutlikkuse suurendamine ja pidev täiustamine

IHR esitab aruande kõigi turvaintsidentide kohta kolmandale eskalatsioonitasemele. See eskalatsioonitase kasutab aruandeid selleks, et teha kindlaks järgmine:

- nõrgad kohad turvakontrollis ja/või käituses, mida tuleb parandada;
- võimalik vajadus seda menetlust tõhustada, et suurendada selle tulemuslikkust intsidentide lahendamisel;

- koolitus- ja suutlikkuse suurendamise võimalused, et veelgi suurendada registrisüsteemide infoturbealast vastupidavust, vähendada uute intsidentide ohtu ja minimeerida nende mõju.

10. INFOTURBE HALDUS

Infoturbe halduse eesmärk on tagada organisatsiooni salastatud teabe, andmete ja IT-teenuste konfidentsiaalsus, terviklus ja käideldavus. Lisaks tehnilistele komponentidele, sealhulgas nende kavandamisele ja testimisele (vt ühenduse tehniline standard), on ajutise lahenduse turvanõuete täitmiseks vaja järgmisi ühiseid töömenetlusi.

10.1. Tundliku teabe kindlakstegemine

Teabe tundlikkuse hindamiseks tehakse kindlaks selle teabega seotud turvarikkumise võimalik mõju ettevõttele (nt rahaline kahju, mainekahju, seaduse rikkumine jne).

Tundlik teabevara tehakse kindlaks selle põhjal, milline on asjaomase vara mõju registritevahelisele ühendusele.

Kõnealuse teabe tundlikkuse taset hinnatakse vastavalt kõnealuse ühenduse suhtes kohaldatavale tundlikkusskaalale, mida on kirjeldatud käesoleva dokumendi osas „Turvaintsidendi käsitlemine“.

10.2. Teabevarade tundlikkustasemed

Teabevara liigitamisel kohaldatakse järgmisi reegleid:

- vähemalt ühe KÕRGE konfidentsiaalsus-, terviklus- või käideldavustaseme kindlakstegemise korral liigitub vara tundlikkustaseme KRIITILINE HKS alla;

- vähemalt ühe KESKMISE konfidentsiaalsus-, terviklus- või käideldavustaseme kindlakstegemise korral liigitub vara tundlikkustaseme TUNDLIK HKS alla;
- üksnes MADALATE konfidentsiaalsus-, terviklus- või käideldavustasemete kindlakstegemise korral liigitub vara tundlikkustaseme PIIRATUD HKS alla.

10.3. Teabevara omaniku määramine

Kõigil teabevaradel peaks olema määratud omanik. HKSi teabevarad, mis kuuluvad ELi tehingulogi ja Šveitsi täiendava tehingulogi vahelisele ühendusele või on sellega seotud, tuleks lisada ühisesse varaloendisse, mida peavad mõlemad lepinguosalised. HKSi teabevarad, mis ei ole seotud ELi tehingulogi ja Šveitsi täiendava tehingulogi vahelise ühendusega, tuleks lisada varaloendisse, mida peab vastav lepinguosaline.

ELi tehingulogi ja Šveitsi täiendava tehingulogi vahelisele ühendusele kuuluva või sellega seotud teabevara omanik määratakse lepinguosaliste kokkuleppel. Teabevara omanik vastutab selle tundlikkuse hindamise eest.

Omanikul peaks olema piisavalt kõrge ametikoht, mis on vastavuses määratud vara(de) väärtusega. Tuleks kokku leppida ja ametlikult vormistada omaniku vastutus vara(de) eest ning kohustus säilitada nõutav konfidentsiaalsuse, tervikluse ja käideldavuse tase.

10.4. Tundliku teabe registreerimine

Kogu tundlik teave registreeritakse tundliku teabe loetelus.

Vajaduse korral võetakse arvesse tundliku teabe koondamist, millel võib olla suurem mõju kui ühel teabeüksusel eraldi, ning see registreeritakse tundliku teabe loetelus (nt süsteemi andmebaasis säilitatava teabe kogum).

Tundliku teabe loetelu ei ole muutumatu. Varadega seotud ohud, haavatavus, turvaintsidentide tõenäosus või tagajärjed võivad muutuda ootamatult ning registrisüsteemidesse võidakse lisada uusi varasid.

Seetõttu vaadatakse tundliku teabe loetelu korrapäraselt läbi ja kõik tundlikuks tunnistatud uued andmed registreeritakse selles viivitamata.

Tundliku teabe loetelu sisaldab iga kirje kohta vähemalt järgmist teavet:

- teabe kirjeldus;
- teabe omanik;
- tundlikkustase;
- märge selle kohta, kas teave sisaldab isikuandmeid;
- vajaduse korral lisateave.

10.5. Tundliku teabe käitlemine

Kui tundlikku teavet töödeldakse väljaspool liidu registri ja Šveitsi registri vahelist ühendust, käideldakse seda vastavalt käitlemisjuhistele.

Liidu registri ja Šveitsi registri vahelise ühenduse kaudu töödeldavat tundlikku teavet käideldakse vastavalt lepinguosaliste turvanõuetele.

10.6. Juurdepääsuhaldus

Juurdepääsuhalduse eesmärk on anda volitatud kasutajatele õigus teenust kasutada, vältides samal ajal volitamata kasutajate juurdepääsu. Juurdepääsuhaldust nimetatakse mõnikord ka „õiguste halduseks“ või „identiteedihalduseks“.

Ajutise lahenduse ja selle toimimise jaoks on mõlemal lepinguosalisel vaja juurdepääsu järgmistele komponentidele:

- Viki: koostöökeskkond ühise teabe vahetamiseks, näiteks väljalaske planeerimise kohta;
- IT-teenuste haldusvahend intsidendi- ja probleemihalduseks (vt peatükk „Lähenemisviis ja standardid“);
- sõnumivahetussüsteem: kumbki lepinguosaline tagab tehinguandmeid sisaldavate sõnumite edastamiseks turvalise sõnumivahetussüsteemi.

Šveitsi registri haldaja ja liidu põhihaldaja tagavad, et juurdepääsuõigused on ajakohased, ning nad on oma osalistele kontaktpunktiks juurdepääsuhaldusega seotud küsimustes. Juurdepääsutaotlusi käsitletakse vastavalt teenindussoovi täitmise menetlustele.

10.7. Sertifikaadi-/võtmehaldus

Kumbki lepinguosaline vastutab oma sertifikaadi-/võtmehalduse eest (sertifikaatide/võtmete genereerimine, registreerimine, talletamine, paigaldamine, kasutamine, uuendamine, tühistamine, varundamine ja taastamine). Nagu on kirjeldatud ühenduse tehnilises standardis (ÜTS), kasutatakse ainult selliseid digitaalseid sertifikaate, mille on väljastanud mõlema lepinguosalise poolt usaldusväärseks peetav sertifitseerimisasutus. Sertifikaatide/võtmete käitlemisel ja talletamisel tuleb järgida käitlemisjuhiseid.

Sertifikaatide ja võtmete tühistamist ja/või uuendamist koordineerivad mõlemad lepinguosalised. Seda tehakse vastavalt teenindussoovi täitmise menetlustele.

Šveitsi registri haldaja ja liidu põhihaldaja vahetavad sertifikaate/võtmeid turvaliste sidevahendite kaudu vastavalt käitlemisjuhistele.

Igasugune sertifikaatide/võtmete kontrollimine lepinguosaliste vahel toimub ribaväliselt.