EUROPESE
COMMISSIE

Brussel, 23.6.2020
COM(2020) 255 final

ANNEX

BIJLAGE

bij

Voorstel voor een besluit van de Raad

betreffende het standpunt dat namens de Europese Unie moet worden ingenomen in het Gemengd Comité dat is opgericht bij de Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten, wat de vaststelling van gemeenschappelijke operationele procedures betreft

BESLUIT Nr. 1/2020 VAN HET GEMENGD COMITÉ DAT IS OPGERICHT BIJ DE OVEREENKOMST TUSSEN DE EUROPESE UNIE EN DE ZWITSERSE BONDSSTAAT INZAKE DE KOPPELING VAN HUN REGELINGEN VOOR DE HANDEL IN BROEIKASGASEMISSIERECHTEN

van ...

betreffende gemeenschappelijke operationele procedures

HET GEMENGD COMITÉ,

Gezien de Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten[1] (hierna "de overeenkomst"), en met name artikel 3,

Overwegende hetgeen volgt:

(1) Bij Besluit nr. 2/2019 van het Gemengd Comité van 5 december 2019 zijn de bijlagen I en II bij de overeenkomst gewijzigd waardoor de in de overeenkomst gestelde voorwaarden voor de koppeling zijn vervuld.

(2) Na de vaststelling van Besluit nr. 2/2019 van het Gemengd Comité en overeenkomstig artikel 21, lid 3, van de overeenkomst hebben de partijen hun akten van ratificatie of goedkeuring uitgewisseld, aangezien zij van oordeel zijn dat alle in de overeenkomst gestelde voorwaarden voor de koppeling zijn vervuld.

(3) Overeenkomstig artikel 21, lid 4, van de overeenkomst is de overeenkomst op 1 januari 2020 in werking getreden.

(4) Overeenkomstig artikel 3, lid 6, van de overeenkomst moeten de Zwitserse registeradministrateur en de centrale administrateur van de Unie voor technische of andere kwesties de voor de werking van de koppeling tussen het EU-transactielogboek (EUTL) van het register van de Unie en het Zwitserse aanvullende transactielogboek (SSTL) vereiste gemeenschappelijke operationele procedures vaststellen en daarbij rekening houden met de prioriteiten van de nationale wetgeving. De gemeenschappelijke operationele procedures moeten in werking treden wanneer zij bij besluit van het Gemengd Comité zijn vastgesteld.

(5) Overeenkomstig artikel 13, lid 1, van de overeenkomst moet het Gemengd Comité technische richtsnoeren overeenkomen voor de correcte uitvoering van de overeenkomst, met inbegrip van richtsnoeren betreffende technische of andere kwesties die voor de werking van de koppeling vereist zijn, daarbij rekening houdend met de prioriteiten van de nationale wetgeving. Technische richtsnoeren kunnen worden ontwikkeld door een overeenkomstig artikel 12, lid 5, van de overeenkomst opgerichte werkgroep. De werkgroep moet ten minste de Zwitserse registeradministrateur en de centrale administrateur van het EU-register omvatten en moet het Gemengd Comité bijstaan in zijn functies uit hoofde van artikel 13 van de overeenkomst.

(6) Gezien de technische aard van de richtsnoeren en de noodzaak deze aan te passen aan de lopende ontwikkelingen, moeten de technische richtsnoeren die door de Zwitserse registeradministrateur en de centrale administrateur van de Unie zijn ontwikkeld, ter informatie of, in voorkomend geval, ter goedkeuring aan het Gemengd Comité worden voorgelegd,

[1] PB L 322 van 7.12.2017, blz. 3.

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

De aan dit besluit gehechte gemeenschappelijke operationele procedures worden vastgesteld.

Artikel 2

Overeenkomstig artikel 12, lid 5, van de overeenkomst wordt hierbij een werkgroep opgericht. De werkgroep assisteert het Gemengd Comité ter waarborging van de correcte uitvoering van de overeenkomst, met inbegrip van de ontwikkeling van technische richtsnoeren voor de uitvoering van de gemeenschappelijke operationele procedures.

De werkgroep omvat ten minste de Zwitserse registeradministrateur en de centrale administrateur van de Unie.

Artikel 3

Dit besluit treedt in werking op de datum waarop het wordt vastgesteld.

Opgemaakt in het Engels te Brussel op XX 2020.

Voor het Gemengd Comité

Secretaris voor de Europese Unie	*De voorzitter*	*Secretaris voor Zwitserland*

AANHANGSEL

BIJLAGE

GEMEENSCHAPPELIJKE OPERATIONELE PROCEDURES (GOP)

uit hoofde van artikel 3, lid 6, van de overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten
- procedures voor voorlopige oplossing -

1. VERKLARENDE WOORDENLIJST

Tabel 1-1 Acroniemen en definities

Acroniem/term	Definitie
Certificeringsautoriteit (CA)	Entiteit die digitale certificaten uitgeeft
CH	Zwitserse Bondsstaat
ETS	Emissiehandelssysteem/emissiehandelsregeling
EU	Europese Unie
IMT	Incidentbeheerteam
Informatiebestanddeel	Informatie die waardevol is voor een bedrijf of organisatie
IT	Informatietechnologie
ITIL	Information Technology Infrastructure Library
ITSM	IT-servicebeheer
LTS	Koppelingstechnische normen
Register	Een boekhoudsysteem voor emissierechten die zijn verleend in het kader van de ETS, waarin eigendom van rechten in elektronische accounts wordt bijgehouden
RFC	Verzoek om wijziging
SIL	Lijst van gevoelige informatie
SR	Verzoek om dienstverlening
Wiki	Website waarop gebruikers informatie en kennis kunnen uitwisselen door inhoud rechtstreeks via een webbrowser aan te vullen of te wijzigen

2. INLEIDING

De Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten van 23 november 2017 (hierna "de overeenkomst" genoemd) voorziet in de wederzijdse erkenning van emissierechten die in het kader van het emissiehandelssysteem van de Europese Unie ("EU-ETS") of de emissiehandelsregeling van Zwitserland ("ETS van Zwitserland") kunnen worden gebruikt. Om de koppeling tussen het EU-ETS en de ETS van Zwitserland operationeel te maken, wordt een directe koppeling tussen het EU-transactielogboek (EUTL) van het register van de Unie en het Zwitserse aanvullende transactielogboek (SSTL) van het Zwitserse register tot stand gebracht, waardoor onder een van beide regelingen verleende emissierechten van de ene naar de andere ETS zullen kunnen worden overgedragen (artikel 3, lid 2, van de overeenkomst). Om de koppeling tussen het EU-ETS en de ETS van Zwitserland operationeel te maken, wordt tegen mei 2020 of zo spoedig mogelijk daarna in een voorlopige oplossing voorzien. De partijen werken samen om de voorlopige oplossing zo spoedig mogelijk door een permanente registerkoppeling te vervangen (bijlage II bij de overeenkomst).

Overeenkomstig artikel 3, lid 6, van de overeenkomst stellen de Zwitserse registeradministrateur en de centrale administrateur van de Unie voor technische of andere kwesties de voor de werking van de koppeling vereiste gemeenschappelijke operationele procedures vast en houden zij daarbij rekening met de prioriteiten van de nationale wetgeving. De door de administrateurs ontwikkelde gemeenschappelijke operationele procedures treden in werking wanneer zij bij besluit van het Gemengd Comité zijn vastgesteld.

De in dit document opgenomen GOP moeten door het Gemengd Comité bij Besluit nr. 1/2020 worden vastgesteld. Overeenkomstig dat besluit verzoekt het Gemengd Comité de Zwitserse registeradministrateur en de centrale administrateur van de Unie om verdere technische richtsnoeren te ontwikkelen om de link te realiseren en ervoor te zorgen dat deze voortdurend worden aangepast aan de technische vooruitgang en aan nieuwe eisen met betrekking tot de veiligheid en beveiliging van de verbinding en tot de doeltreffende en efficiënte werking ervan.

2.1. Toepassingsgebied

Dit document omvat het akkoord tussen de partijen bij de overeenkomst over de totstandbrenging van de procedurele grondslag van de koppeling tussen de registers van het EU-ETS en de ETS van Zwitserland. In het document worden de algemene procedurele vereisten inzake de werking van de koppeling uiteengezet. Om de koppeling te realiseren moeten echter verdere technische richtsnoeren worden vastgesteld.

Voor de goede werking van de koppeling zullen technische specificaties nodig zijn om de koppeling verder te realiseren. Overeenkomstig artikel 3, lid 7, van de overeenkomst worden deze kwesties in detail beschreven in het document betreffende koppelingstechnische normen, dat afzonderlijk bij besluit van het Gemengd Comité moet worden aangenomen.

Het doel van de GOP is ervoor te zorgen dat IT-diensten die verband houden met de werking van de koppeling tussen de registers van het EU-ETS en de ETS van Zwitserland, effectief en efficiënt worden geleverd, met name voor het inwilligen van verzoeken om dienstverlening, het oplossen van storingen en van problemen en het uitvoeren van routinetaken overeenkomstig internationale normen voor het beheer van IT-diensten.

Voor de overeengekomen voorlopige oplossing zijn alleen de volgende GOP nodig, die in dit document zijn opgenomen:

- incidentbeheer;
- probleembeheer;
- inwilliging van verzoeken;
- wijzigingsbeheer;
- releasebeheer;
- beheer van beveiligingsincidenten;
- beheer van informatiebeveiliging.

Met de uitrol van de permanente registerkoppeling op een later tijdstip moeten de GOP waar nodig worden aangepast en aangevuld.

2.2. Adressaten

De doelgroep van deze GOP zijn de teams voor ondersteuning van de registers van de EU en Zwitserland.

3. AANPAK EN NORMEN

Het volgende beginsel is van toepassing op alle GOP:

- De EU en CH komen overeen de GOP te definiëren op basis van ITIL (Information Technology Infrastructure Library, versie 3). De praktijken van deze norm worden hergebruikt en aangepast aan de specifieke behoeften in verband met de voorlopige oplossing.
- De voor de verwerking van de GOP benodigde communicatie en coördinatie tussen de twee partijen vindt plaats via de servicedesks van de registers van CH en de EU. Taken worden altijd toegewezen binnen één partij.
- Indien er onenigheid bestaat over de behandeling van een GOP, wordt dit geanalyseerd en tussen de beide servicedesks opgelost. Indien geen overeenstemming kan worden bereikt, wordt het vinden van een gezamenlijke oplossing geëscaleerd naar een hoger niveau.

Escalatieniveaus	**EU**	**CH**
1e niveau	EU-servicedesk	CH-servicedesk
2e niveau	Operationeel manager van de EU	Applicatiemanager van CH
3e niveau	Gemengd Comité (dat deze verantwoordelijkheid kan delegeren overeenkomstig artikel 12, lid 5, van de overeenkomst)	
4e niveau	Gemengd Comité, indien 3e niveau is gedelegeerd	

- Elke partij kan de procedures voor de werking van haar eigen registratiesysteem vaststellen, rekening houdend met de eisen en interfaces van deze GOP.
- Het instrument voor IT-beheer (IT Service Management, ITSM) wordt gebruikt ter ondersteuning van de GOP, met name het beheer van incidenten, het beheer van problemen en het inwilligen van verzoeken, en de communicatie tussen beide partijen.

- Bovendien is de uitwisseling van informatie via e-mail toegestaan.
- Beide partijen zorgen ervoor dat de voorschriften voor de beveiliging van de informatie overeenkomstig de instructies voor de behandeling ervan worden nageleefd.

4. INCIDENTBEHEER

Het doel van het incidentbeheerproces is om de normale werking van de IT-diensten zo snel mogelijk en met minimale verstoring te herstellen.

Incidentbeheer moet ook een register bijhouden van incidenten voor rapportagedoeleinden en met andere processen integreren om voortdurende verbetering te stimuleren.

- Incidentbeheer omvat algemeen gezien de volgende activiteiten:
- opsporing en registratie van incidenten;
- classificatie en initiële ondersteuning;
- onderzoek en diagnose;
- oplossing en herstel;
- afsluiting van het incident.

Gedurende de loop van een incident is het incidentbeheer verantwoordelijk voor de eigendom, monitoring, tracering en communicatie.

4.1. Opsporing en registratie van incidenten

Een incident kan worden opgespoord door een ondersteuningsgroep, door geautomatiseerde monitoringinstrumenten of door technisch personeel dat routinematig toezicht uitvoert.

Na opsporing moet een incident worden geregistreerd en moet er een unieke identificatiecode worden toegewezen waarmee het incident kan worden gevolgd en gemonitord. De unieke identificatiecode van een incident is de identificatiecode die in het gemeenschappelijk ticketsysteem is toegekend door de servicedesk van de partij (EU of CH) die het incident heeft gemeld, en moet in elke communicatie over het incident worden gebruikt.

Voor alle incidenten is het contactpunt de servicedesk van de partij die het ticket heeft geregistreerd.

4.2. Classificatie en initiële ondersteuning

Het incident moet worden geclassificeerd om te begrijpen en te bepalen welk systeem en/of welke dienst bij het incident betrokken zijn en in welke mate. Voor een doeltreffende werking moet de classificatie het incident bij de eerste poging naar de juiste dienstverlener leiden om te zorgen voor een snelle oplossing van het incident.

In de classificatiefase moeten de categorie en prioriteit van het incident worden bepaald op basis van de impact en urgentie ervan, zodat het kan worden behandeld binnen een termijn die overeenstemt met de prioriteit.

Indien het incident mogelijk gevolgen heeft voor de vertrouwelijkheid of integriteit van gevoelige gegevens en/of een impact heeft op de beschikbaarheid van het systeem, moet het incident ook worden aangemerkt als een beveiligingsincident en vervolgens worden behandeld volgens het proces dat is vastgesteld in het hoofdstuk “Beheer van beveiligingsincidenten”.

Indien mogelijk verricht de servicedesk die het ticket heeft geregistreerd een eerste diagnose. Hiervoor zal de servicedesk nagaan of het incident een bekende fout is. Als dat het geval is, is de werkwijze voor de oplossing of workaround al bekend en gedocumenteerd.

Indien de servicedesk erin slaagt het incident op te lossen, dan wordt het incident bij deze stap afgesloten, aangezien is voldaan aan het hoofddoel van het incidentbeheer (namelijk het snelle herstel van de dienst voor de eindgebruiker). Indien dit niet het geval is, escaleert de servicedesk het incident naar de desbetreffende werkgroep voor verder onderzoek en diagnose.

4.3. Onderzoek en diagnose

Onderzoek en diagnose van incidenten wordt toegepast wanneer een incident niet kan worden opgelost door de servicedesk als onderdeel van de initiële diagnose, en daarom wordt geëscaleerd naar het passende niveau. De escalatie van een incident maakt integraal deel uit van het onderzoeks- en diagnoseproces.

Een gangbare praktijk in de onderzoeks- en diagnosefase is te trachten om het incident onder gecontroleerde omstandigheden te reproduceren. Bij onderzoek en diagnose is het belangrijk dat een goed begrip wordt gevormd van de volgorde van de gebeurtenissen die aan het incident vooraf gingen.

Escalatie is de erkenning dat een incident niet op het huidige steunniveau kan worden opgelost en moet worden doorgegeven aan een ondersteunende groep op een hoger niveau of aan de andere partij. De escalatie kan op twee manieren verlopen: horizontaal (functioneel) of verticaal (hiërarchisch).

De servicedesk die het incident heeft geregistreerd en geactiveerd, is verantwoordelijk voor het escaleren van het incident naar de juiste dienstverlener en voor het volgen van de algemene status en de toewijzing van het incident.

De partij waaraan het incident is toegewezen, is verantwoordelijk voor de tijdige uitvoering van de gevraagde maatregelen en voor het geven van feedback aan de servicedesk van de eigen partij.

4.4. Oplossing en herstel

De oplossing van incidenten en het herstel vindt plaats zodra een volledig begrip van het incident is gevormd. Het vinden van een oplossing voor een incident betekent dat er een manier is gevonden om het probleem te corrigeren. De handeling waarbij de oplossing wordt uitgevoerd, is de herstelfase.

Zodra de desbetreffende dienstverleners het uitvallen van de dienst hebben verholpen, wordt het incident teruggeleid naar de desbetreffende servicedesk die het incident heeft geregistreerd, en die bij de melder van het incident bevestigd dat de fout is hersteld en dat het incident kan worden afgesloten. De bevindingen van de verwerking van het incident moeten voor toekomstig gebruik worden geregistreerd.

Het herstel kan worden uitgevoerd door IT-ondersteunend personeel of door het verstrekken van een reeks instructies aan de eindgebruiker.

4.5. Afsluiting van het incident

Afsluiting is de laatste stap in het incidentbeheer en vindt plaats kort na de oplossing van het incident.

Van de checklist van activiteiten die tijdens de afsluitingsfase moeten worden uitgevoerd, wordt het volgende benadrukt:

- de verificatie van de initiële categorisering van het incident;
- de juiste registratie van alle informatie over het incident;
- de juiste documentatie van het incident en de bijwerking van de kennisbasis;
- de juiste communicatie met alle belanghebbenden die direct of indirect door het incident zijn getroffen.

Een incident wordt formeel gesloten zodra de fase van de afsluiting van de incidenten door de servicedesk is uitgevoerd en aan de andere partij is meegedeeld.

Zodra een incident is afgesloten, wordt het niet heropend. Als een incident zich binnen een korte periode opnieuw voordoet, wordt het oorspronkelijke incident niet opnieuw geopend, maar moet een nieuw incident worden geregistreerd.

Indien het incident wordt gevolgd door de servicedesks van zowel de EU als CH, is de definitieve afsluiting de verantwoordelijkheid van de servicedesk die het ticket heeft geregistreerd.

5. PROBLEEMBEHEER

Deze procedure moet worden gevolgd wanneer een probleem wordt vastgesteld en derhalve het proces voor probleembeheer in gang zet. Probleembeheer is gericht op het verbeteren van de kwaliteit en het verminderen van het aantal gemelde incidenten. Een probleem kan de oorzaak zijn van een of meer incidenten. Wanneer een incident wordt gemeld, is het doel van het incidentbeheer om de dienst zo snel mogelijk te herstellen, waarbij workarounds nodig kunnen zijn. Wanneer een probleem wordt geconstateerd, is het doel de onderliggende oorzaak ervan te onderzoeken om een wijziging te kunnen vaststellen die ervoor zal zorgen dat het probleem en de daarmee samenhangende incidenten niet meer zullen voorkomen.

5.1. Identificatie en registratie van een probleem

Afhankelijk van welke partij het ticket heeft geopend, is de servicedesk van de EU of CH het contactpunt voor alle aan het probleem gerelateerde kwesties.

De unieke identificatiecode van een probleem is de identificatiecode die door het ITSM wordt toegekend. De code moet worden gebruikt in alle communicatie in verband met het probleem.

Een probleem kan worden geactiveerd door een incident, of kan op eigen initiatief worden geopend om een oplossing te vinden voor problemen die in eender welke fase in het systeem worden geconstateerd.

5.2. Prioritering van problemen

Problemen kunnen op dezelfde wijze als incidenten worden gecategoriseerd op basis van de ernst en prioriteit ervan, om het volgen ervan te vergemakkelijken, rekening houdend met de gevolgen van de betrokken incidenten en de frequentie waarmee zij zich hebben voorgedaan.

5.3. Onderzoek en diagnose van het probleem

Elke partij kan een probleem melden, waarna de servicedesk van de desbetreffende partij verantwoordelijk is voor de registratie ervan, de toewijzing ervan aan de juiste dienstverlener, en het volgen van de algemene status ervan.

Het oplossingsteam waaraan het probleem is geëscaleerd, is verantwoordelijk voor het tijdig behandelen van het probleem en voor de communicatie met de servicedesk.

Na een verzoek zijn beide partijen verantwoordelijk voor de uitvoering van de toegewezen acties en voor het geven van feedback aan de servicedesk van de eigen partij.

5.4. Oplossing

Het oplossingsteam waaraan het probleem is toegewezen, is verantwoordelijk voor het oplossen van het probleem en het verstrekken van relevante informatie aan de servicedesk van de eigen partij.

De bevindingen van de verwerking van het probleem moeten voor toekomstig gebruik worden geregistreerd.

5.5. Afsluiting van een probleem

Een probleem wordt formeel afgesloten zodra het probleem is opgelost door de wijziging door te voeren. De afsluitingsfase wordt uitgevoerd door de servicedesk die het probleem heeft geregistreerd en de servicedesk van de andere partij daarvan in kennis heeft gesteld.

6. INWILLIGING VAN VERZOEKEN

De inwilliging van verzoeken omvat het volledige beheer van een verzoek om een nieuwe of bestaande dienst vanaf het moment dat het is geregistreerd en goedgekeurd tot aan de afsluiting ervan. Het gaat meestal om kleine, vooraf gedefinieerde, herhaalbare, frequente, vooraf goedgekeurde en procedurele verzoeken.

Hieronder volgt een overzicht van de belangrijkste stappen die moeten worden ondernomen.

6.1. Initiatie van het verzoek

De informatie met betrekking tot een verzoek om dienstverlening wordt per e-mail, per telefoon, of via het ITSM of een ander overeengekomen communicatiekanaal bij de servicedesk van de EU of CH ingediend.

6.2. Registratie en analyse van het verzoek

Voor alle verzoeken om dienstverlening moet het contactpunt de EU- of CH-servicedesk zijn, afhankelijk van welke partij het verzoek heeft ingediend. Deze servicedesk is verantwoordelijk voor het bijhouden en analyseren van het verzoek om dienstverlening en de passende zorgvuldigheid.

6.3. Goedkeuring aanvragen

De medewerker van de servicedesk van de partij die het verzoek om dienstverlening heeft ingediend, controleert of er goedkeuring van de andere partij nodig is, en zo ja, verkrijgt deze. Indien het verzoek om dienstverlening niet wordt goedgekeurd, wordt het ticket door de servicedesk geactualiseerd en afgesloten.

6.4. Inwilliging van het verzoek

Deze stap is gericht op een doeltreffende en efficiënte afhandeling van de verzoeken om dienstverlening. Hierbij worden de volgende categorieën gehanteerd:

- de uitvoering van de dienst heeft voor slechts één gevolgen. In dit geval geeft deze partij de werkopdrachten en coördineert zij de uitvoering;
- de uitvoering van de dienst heeft gevolgen voor zowel EU als CH. In dit geval geven de servicedesks van de werkopdrachten op hun bevoegdheidsgebied. De verwerking van de inwilliging van het verzoek wordt tussen beide servicedesks

gecoördineerd. De algemene verantwoordelijkheid ligt bij de servicedesk die het verzoek heeft ontvangen en geïnitieerd.

Wanneer het verzoek om dienstverlening is ingewilligd, moet het de status "opgelost" worden gegeven.

6.5. Escalatie van een verzoek

De servicedesk kan het lopende verzoek om dienstverlening, indien nodig, naar de juiste dienstverlener escaleren (derde partij).

Escalaties worden uitgevoerd aan de respectieve derde partijen, dat wil zeggen dat de EU-servicedesk via de CH-servicedesk voor escalatie naar een derde CH-partij zal moeten gaan, en omgekeerd.

De derde partij waaraan het verzoek geëscaleerd is, is verantwoordelijk voor de tijdige behandeling van het verzoek en voor de communicatie met de servicedesk die het verzoek heeft geëscaleerd.

De servicedesk die het verzoek om dienstverlening heeft aangemeld, is verantwoordelijk voor het traceren van de algemene status en de toewijzing van een verzoek om dienstverlening.

6.6. Herziening van de inwilliging van het verzoek

De verantwoordelijke servicedesk onderwerpt de registratie van het verzoek om dienstverlening aan een laatste kwaliteitscontrole voordat het wordt afgesloten. Het doel daarvan is om er zeker van te zijn dat een verzoek om dienstverlening daadwerkelijk wordt verwerkt en dat alle informatie die nodig is om de levenscyclus van het verzoek te beschrijven, voldoende gedetailleerd wordt verstrekt. Daarnaast moeten de bevindingen van de verwerking van het verzoek worden geregistreerd voor toekomstig gebruik.

6.7. Afsluiting van het verzoek

Indien de aangewezen partijen overeenkomen dat het verzoek om dienstverlening is ingewilligd en de verzoeker van mening is dat de zaak is opgelost, wordt de status veranderd in "Afgesloten".

Een verzoek om dienstverlening is formeel afgesloten zodra de servicedesk die het dienstverzoek heeft geregistreerd, de afsluitingsfase heeft uitgevoerd en de servicedesk van de andere partij daarvan in kennis heeft gesteld.

7. WIJZIGINGSBEHEER

Het doel is ervoor te zorgen dat gestandaardiseerde methoden en procedures worden gebruikt voor een efficiënte en snelle afhandeling van alle wijzigingen van de IT-infrastructuur, teneinde het aantal van eventuele gerelateerde incidenten en de gevolgen daarvan voor de dienstverlening tot een minimum te beperken. Wijzigingen in de IT-infrastructuur kunnen zich voordoen als reactie op problemen of extern opgelegde vereisten, bijvoorbeeld wijzigingen van de wetgeving, of proactief met het oog op meer efficiëntie en doeltreffendheid of om zakelijke initiatieven mogelijk te maken of te weerspiegelen.

Het wijzigingsbeheer omvat verschillende stappen die alle details van een wijzigingsverzoek opslaan voor toekomstige tracering. Deze processen zorgen ervoor dat de wijziging gevalideerd en getest wordt alvorens te worden doorgevoerd. Releasebeheer is verantwoordelijk voor de succesvolle uitrol van de wijziging.

7.1. Verzoek om wijziging

Een verzoek om wijziging (RFC) wordt ter validering en goedkeuring ingediend bij het wijzigingsbeheerteam. Voor alle wijzigingsverzoeken moet het contactpunt de EU- of CH-servicedesk zijn, afhankelijk van welke partij het verzoek heeft ingediend. Deze servicedesk is verantwoordelijk voor het registreren en analyseren van het verzoek met de nodige zorgvuldigheid.

Wijzigingsverzoeken kunnen voortkomen uit:

- een incident dat een wijziging veroorzaakt;
- een bestaand probleem dat tot een wijziging leidt;
- een eindgebruiker die om een nieuwe wijziging verzoekt;
- een wijziging als gevolg van een lopend onderhoud;
- wijzigingen in de wetgeving.

7.2. Evaluatie en planning van wijzigingen

In deze fase worden de beoordelings- en planningsactiviteiten behandeld. De fase omvat prioritering en planningsactiviteiten om de risico's en de impact tot een minimum te beperken.

Indien de uitvoering van het wijzigingsverzoek gevolgen heeft voor zowel de EU als CH, verifieert de partij die het verzoek heeft aangemeld, de evaluatie en planning van de wijziging met de andere partij.

7.3. Goedkeuring van wijzigingen

Elk geregistreerd wijzigingsverzoek moet door het desbetreffende escalatieniveau worden goedgekeurd.

7.4. Uitvoering van de wijziging

De uitvoering van de wijziging wordt verwerkt in releasebeheer. De releasebeheerteams van beide partijen volgen hun eigen processen met betrekking tot planning en tests. Herziening vindt plaats zodra de uitvoering is voltooid. Om er zeker van te zijn dat alles volgens plan is verlopen, wordt het bestaande proces van wijzigingsbeheer voortdurend geëvalueerd en waar nodig geactualiseerd.

8. RELEASEBEHEER

Onder release wordt een of meer wijzigingen in een IT-dienst verstaan die worden verzameld in een releaseplan, en samen worden goedgekeurd, voorbereid, gebouwd, getest en uitgevoerd. Een release kan de oplossing van een bug omvatten, of een wijziging van de hardware of andere onderdelen, wijziging van de software, upgrades van applicaties, wijzigingen van de documentatie en/of processen. De inhoud van elke release wordt als een enkele entiteit beheerd, getest en ingezet.

Releasebeheer is gericht op het plannen, bouwen, testen en valideren van en het leveren van de capaciteit voor het verlenen van de diensten, die de eisen van de belanghebbenden zullen vervullen en de beoogde doelstellingen zullen verwezenlijken. De acceptatiecriteria voor alle wijzigingen van de dienst zullen worden vastgesteld en gedocumenteerd bij de coördinatie van het ontwerp en worden verstrekt aan de releasebeheerteams.

De release bestaat doorgaans uit een aantal oplossingen van problemen en verbeteringen van een dienst. De release omvat de vereiste nieuwe of veranderde software en de nieuwe of veranderde hardware die nodig is om de goedgekeurde wijzigingen uit te voeren.

8.1. Plannen van de release

In de eerste stap van het proces worden geautoriseerde wijzigingen aan releasepaketten toegewezen en worden het toepassingsgebied en de inhoud van de releases bepaald. Op basis van deze informatie ontwikkelt het subproces van de releaseplanning een tijdschema voor de opbouw, het testen en het inzetten van de release.

Bij de planning moet het volgende worden bepaald:

- toepassingsgebied en inhoud van de release;
- risicobeoordeling en risicoprofiel voor de release;
- de door de release getroffen klant/gebruikers;
- team dat verantwoordelijk is voor de release;
- strategie voor uitvoering en uitrol;
- middelen voor de release en uitrol ervan.

Beide partijen brengen elkaar op de hoogte van de planning van releases en onderhoudsvensters. Indien een release gevolgen heeft voor zowel de EU als CH, coördineren zij de planning en stellen zij een gemeenschappelijk onderhoudsvenster vast.

8.2. Bouwen en testen van releasepakket

Bij de bouw- en teststap van het releasebeheerproces wordt de benadering vastgesteld van de uitvoering van de release of het releasepakket en van de handhaving van de gecontroleerde omgeving voorafgaand aan de wijziging van de productie, alsmede het testen van alle wijzigingen van de release in alle omgevingen.

Indien een release gevolgen heeft voor zowel de EU als CH, coördineren zij de releaseplanning en de tests. Hierbij komen de volgende aspecten aan bod:

- hoe en wanneer release-units en dienstencomponenten zullen worden geleverd;
- wat de typische aanlooptijd is; wat er gebeurt in geval van een vertraging;
- hoe wordt de voortgang van de levering bijgehouden en bevestiging verkregen;
- maatstaven voor monitoring en bepaling van het succes van de uitrol van de release;
- gemeenschappelijke testcases voor relevante functies en wijzigingen.

Aan het eind van dit subproces zijn alle voorgeschreven onderdelen klaar voor de uitrolfase.

8.3. Voorbereiden van uitrol

Door het voorbereidingssubproces wordt gewaarborgd dat de communicatieplannen correct zijn gedefinieerd en de kennisgevingen klaar zijn om te worden toegezonden aan alle belanghebbenden en eindgebruikers, en dat de release wordt geïntegreerd in het proces van wijzigingsbeheer om ervoor te zorgen dat alle wijzigingen op een gecontroleerde manier worden uitgevoerd en door de vereiste fora worden goedgekeurd.

Indien een release gevolgen heeft voor zowel de EU als CH, coördineren zij de volgende activiteiten.

- Wijzigingsaanvragen registreren voor planning en voorbereiding van release in de productieomgeving;
- opstellen van het uitvoeringsplan;
- een aanpak voor eventuele terugdraaiing, zodat in geval van een mislukte uitrol terug kan worden gekeerd naar de vorige staat;
- kennisgevingen die aan alle noodzakelijke partijen worden gezonden;
- goedkeuring vragen voor de uitvoering van de release van het desbetreffende escalatieniveau.

8.4. Terugdraaien van de release

Indien de uitrol is mislukt of indien bij de tests is geconstateerd dat de uitrol niet succesvol is of niet voldoet aan de vastgestelde acceptatie- of kwaliteitscriteria, dan moeten de releasebeheerteams van beide partijen de uitrol terugdraaien. Alle noodzakelijke belanghebbenden moeten worden geïnformeerd, met inbegrip van de getroffen/beoogde eindgebruikers. In afwachting van goedkeuring kan het proces in elk van de vorige fasen opnieuw worden gestart.

8.5. Herziening en afsluiting van de release

Bij de herziening van een uitrol moeten de volgende activiteiten worden opgenomen:

- het verzamelen van feedback over de tevredenheid van klanten, gebruikers en diensten met de uitrol (verzamelen en bestuderen van de feedback voor de voortdurende verbetering van de dienst);
- kwaliteitscriteria waaraan niet is voldaan, herzien;
- controleren of alle maatregelen, noodzakelijke correcties en de wijzigingen zijn afgerond;
- ervoor zorgen dat er aan het einde van de uitrol geen problemen op het gebied van capaciteit, middelen of prestaties zijn;
- verifiëren dat eventuele problemen, bekende fouten en workarounds worden gedocumenteerd en aanvaard door de klant, de eindgebruikers, de operationele ondersteuning en andere betrokken partijen;
- toezicht houden op incidenten en problemen die het gevolg zijn van de uitrol (het verlenen van steun in de beginfase aan operationele teams indien de release leidt tot een toename van de hoeveelheid werk);
- bijwerken van de ondersteunende documentatie (d.w.z. technische informatiedocumenten);
- de uitrol van de release formeel overdragen aan de operationele teams;
- documentatie van geleerde lessen;
- documenten met de samenvatting van de release van de uitvoerende teams verzamelen;
- de release formeel afsluiten na de controle van de registratie van het wijzigingsverzoek.

9. BEHEER VAN BEVEILIGINGSINCIDENTEN

Beheer van beveiligingsincidenten is een proces voor de behandeling van beveiligingsincidenten om de belanghebbenden in staat te stellen informatie over incidenten te verstrekken; evaluatie en prioritering van incidenten; en incidentrespons om een feitelijke, vermeende of mogelijke inbreuk op de vertrouwelijkheid, beschikbaarheid of integriteit van gevoelige informatie te regelen.

9.1. Categorisering van informatiebeveiligingsincidenten

Alle incidenten die van invloed zijn op de koppeling tussen het EU-register en het Zwitserse register worden geanalyseerd om mogelijke inbreuken op de vertrouwelijkheid, de integriteit of de beschikbaarheid van gevoelige informatie op de Lijst van gevoelige informatie (SIL) vast te stellen.

Als dat het geval is, moet het incident worden aangemerkt als een incident op het gebied van informatiebeveiliging, onmiddellijk worden geregistreerd in het ITSM en als zodanig worden beheerd.

9.2. Behandeling van informatiebeveiligingsincidenten

Beveiligingsincidenten vallen onder de verantwoordelijkheid van het 3e escalatieniveau en de oplossing van de incidenten wordt behandeld door een specifiek team voor incidentbeheer (IMT).

Het IMT is verantwoordelijk voor:

- het uitvoeren van een eerste analyse, categoriseren en beoordelen van de ernst van het incident;
- het coördineren van acties tussen alle belanghebbenden, met inbegrip van de volledige documentatie van de analyse van het incident, de besluiten die zijn genomen om het incident aan te pakken en de mogelijke vastgestelde tekortkomingen;
- afhankelijk van de ernst van het beveiligingsincident, de tijdige escalatie naar het juiste niveau voor informatie en/of beslissing.

Bij het beheer van informatiebeveiliging wordt alle informatie betreffende incidenten gerubriceerd op het hoogste niveau van gevoeligheid van de informatie, maar in elk geval niet lager dan ETS SENSITIVE.

Voor een lopend onderzoek en/of een tekortkoming die kan worden misbruikt en tot aan het herstel ervan, wordt de informatie gerubriceerd als ETS CRITICAL.

9.3. Identificatie van beveiligingsincidenten

De informatiebeveiligingsfunctionaris bepaalt op basis van aard van het incident de passende organisaties die moeten worden betrokken en deel moeten uitmaken van het IMT.

9.4. Analyse van beveiligingsincidenten

Het IMT werkt samen met alle betrokken organisaties en de betrokken leden van hun teams, naargelang van het geval, bij de beoordeling van het incident. Tijdens de analyse wordt de mate van het verlies van vertrouwelijkheid, integriteit of beschikbaarheid vastgesteld en worden de gevolgen voor alle betrokken organisaties beoordeeld. Vervolgens worden initiële en follow-upacties vastgesteld om het incident op te lossen en de gevolgen ervan te beheren, met inbegrip van het effect van deze maatregelen op de middelen.

9.5. Beoordeling van de ernst van beveiligingsincidenten, escalatie en rapportage

Het IMT beoordeelt de ernst van een nieuw beveiligingsincident na de categorisering ervan en begint met onmiddellijke maatregelen naargelang de ernst van het incident.

9.6. Rapportage van beveiligingsrespons

Het IMT vermeldt de resultaten van de beperking en het herstel van het incident in het incidentresponsverslag. Het verslag wordt aan het 3e escalatieniveau verstrekt door middel van beveiligde e-mail of andere wederzijds aanvaarde middelen van beveiligde communicatie.

De verantwoordelijke partij evalueert de resultaten van de beperking en het herstel en:

- verbindt het register opnieuw indien de verbinding eerder was verbroken;
- verstrekt incidentmeldingen aan de teams van het register;
- Sluit het incident af.

Het IMT moet — op een veilige manier — relevante details vermelden in het verslag over het informatiebeveiligingsincident, teneinde een consistente registratie en communicatie te waarborgen en een snelle en passende actie mogelijk te maken om het incident te beperken. Het IMT dient het eindverslag over het informatiebeveiligingsincident na voltooiing tijdig in.

9.7. Monitoring, capaciteitsopbouw en continue verbetering

Het IMT brengt voor alle beveiligingsincidenten verslag uit aan het 3e escalatieniveau. De verslagen zullen door dit escalatieniveau worden gebruikt om het volgende te bepalen:

- zwakke punten in de beveiligingscontroles en/of de functionering die moeten worden versterkt;
- de mogelijke behoefte om deze procedure te versterken om de doeltreffendheid van de respons op incidenten te verbeteren;

- Opleiding en capaciteitsopbouw om de informatiebeveiliging van registersystemen verder te versterken, het risico op toekomstige incidenten te verminderen en het effect ervan tot een minimum te beperken.

10. BEHEER VAN INFORMATIEBEVEILIGING

Beheer van informatiebeveiliging heeft ten doel de vertrouwelijkheid, integriteit en beschikbaarheid van de gerubriceerde informatie, gegevens en IT-diensten van een organisatie te waarborgen. Naast de technische onderdelen, met inbegrip van het ontwerp en de tests (zie LTS), zijn de volgende gemeenschappelijke operationele procedures nodig om aan de beveiligingseisen voor de voorlopige oplossing te voldoen.

10.1. Identificatie van gevoelige informatie

De gevoeligheid van informatie wordt beoordeeld aan de hand van de gevolgen voor het bedrijf (bv. financiële verliezen, reputatieschade, schending van het recht...) die een beveiligingsinbreuk in verband met de informatie zou kunnen hebben.

De gevoeligheid van informatie wordt bepaald op basis van het effect ervan op de koppeling.

Het gevoeligheidsniveau van deze informatie wordt beoordeeld aan de hand van de gevoeligheidsschaal die van toepassing is op deze koppeling en nader uitgewerkt in het gedeelte “Behandeling van informatiebeveiligingsincidenten” van dit document.

10.2. Gevoeligheidsniveaus van de informatiebestanddelen

Bij de identificatie wordt een informatiebestanddeel gerubriceerd aan de hand van de volgende regels:

- bij de identificatie van ten minste één HOOG vertrouwelijkheids-, integriteits- of beschikbaarheidsniveau wordt het informatiebestanddeel gerubriceerd als ETS CRITICAL;
- bij de identificatie van ten minste één MIDDELHOOG vertrouwelijkheids-, integriteits- of beschikbaarheidsniveau wordt het informatiebestanddeel gerubriceerd als ETS SENSITIVE;
- bij de identificatie van ten minste één LAAG vertrouwelijkheids-, integriteits- of beschikbaarheidsniveau wordt het informatiebestanddeel gerubriceerd als ETS LIMITED.

10.3. Toewijzing van de eigenaar van het informatiebestanddeel

Alle informatiebestanddelen moeten een toegewezen eigenaar hebben. Informatiebestanddelen van de ETS, die behoren tot of verband houden met de koppeling tussen het EUTL en het SSTL, moeten worden opgenomen in een gezamenlijke inventaris van informatiebestanddelen, die door beide partijen wordt bijgehouden. Informatiebestanddelen van de ETS buiten de koppeling tussen het EUTL en het SSTL moeten worden opgenomen in een inventaris van de bestanddelen, die door de respectieve partij wordt bijgehouden.

De eigendom van elk informatiebestanddeel dat behoort tot of verband houdt met de koppeling tussen het EUTL en de SSTL moet worden overeengekomen door de partijen. De eigenaar van een informatiebestanddeel is verantwoordelijk voor de beoordeling van de gevoeligheid ervan.

De eigenaar moet een anciënniteit hebben die passend is voor de waarde van het toegewezen bestanddeel. De verantwoordelijkheid van de eigenaar voor het bestanddeel en de verplichting om het vereiste niveau van vertrouwelijkheid, integriteit en beschikbaarheid te handhaven, moet worden overeengekomen en geformaliseerd.

10.4. Registratie van gevoelige informatie

Alle gevoelige informatie wordt geregistreerd in de Lijst voor gevoelige informatie (SIL).

In voorkomend geval wordt de samenvoeging van gevoelige informatie die tot een groter effect zou kunnen leiden dan het effect van één enkel informatiebestanddeel, in aanmerking genomen en geregistreerd in de SIL (bv. verzameling van informatie die in de systeemdatabank is opgeslagen).

De SIL is niet statisch. Dreigingen, kwetsbaarheden en de waarschijnlijkheid of gevolgen van beveiligingsincidenten met betrekking tot de informatie kunnen zonder enige indicatie veranderen en nieuwe informatiebestanddelen kunnen worden opgenomen in de registersystemen.

De SIL wordt derhalve regelmatig geëvalueerd en alle nieuwe als gevoelig aangemerkte informatie wordt onmiddellijk in de SIL geregistreerd.

De SIL bevat voor elke vermelding ten minste de volgende gegevens:

- beschrijving van de informatie;
- eigenaar van de informatie;

- gevoeligheidsniveau;
- vermelding of de informatie persoonsgegevens bevat;
- aanvullende informatie, indien nodig.

10.5. Behandeling van gevoelige informatie

Wanneer gevoelige informatie buiten de koppeling tussen het EU-register en het Zwitserse register wordt verwerkt, wordt deze behandeld overeenkomstig de instructies voor de behandeling van gevoelige informatie.

Gevoelige informatie die wordt verwerkt door de koppeling tussen het EU-register en het Zwitserse register wordt behandeld overeenkomstig de beveiligingsvoorschriften van de partijen.

10.6. Toegangsbeheer

Het doel van het toegangsbeheer is geautoriseerde gebruikers het recht te geven gebruik te maken van een dienst, waarbij de toegang voor niet-geautoriseerde gebruikers wordt verhinderd. Toegangsbeheer wordt soms ook "rechtenbeheer" of "identiteitsbeheer" genoemd.

Voor de voorlopige oplossing en de werking ervan hebben beide partijen toegang nodig tot:

- wiki: een samenwerkingsomgeving voor de uitwisseling van gemeenschappelijke informatie, zoals releaseplanning;
- het ITSM voor het beheer van incidenten en problemen (zie het hoofdstuk "Aanpak en normen");
- een systeem voor de uitwisseling van berichten: elke partij voorziet in een beveiligd systeem voor de uitwisseling van berichten waarin de transactiegegevens worden doorgegeven.

De Zwitserse registeradministrateur en de centrale administrateur van de Unie zien erop toe dat de toegangen beschikbaar zijn en fungeren als contactpunten voor hun partijen voor activiteiten op het gebied van toegangsbeheer. Verzoeken om toegang worden behandeld volgens de procedures voor het inwilligen van verzoeken.

10.7. Certificaat-/sleutelbeheer

Elke partij is verantwoordelijk voor haar eigen certificaat-/sleutelbeheer (productie, registratie, opslag, installatie, gebruik, verlenging, intrekking, backup en recuperatie van certificaten/sleutels). Zoals uiteengezet in de koppelingstechnische normen (LTS), worden alleen digitale certificaten gebruikt die zijn afgegeven door een door beide partijen vertrouwde certificeringsautoriteit (CA). Bij de behandeling en opslag van certificaten/sleutels moeten de bepalingen van de instructies voor de behandeling worden gevolgd.

De intrekking en/of verlenging van certificaten en sleutels moet altijd door beide partijen gecoördineerd. Dit gebeurt volgens de procedures voor het inwilligen van verzoeken.

De Zwitserse registeradministrateur en de centrale administrateur van de Unie zullen certificaten/sleutels uitwisselen via beveiligde communicatiemiddelen overeenkomstig de instructies in de instructies voor behandeling.

Eventuele verificatie van certificaten/sleutels tussen de partijen vindt plaats buiten de band.