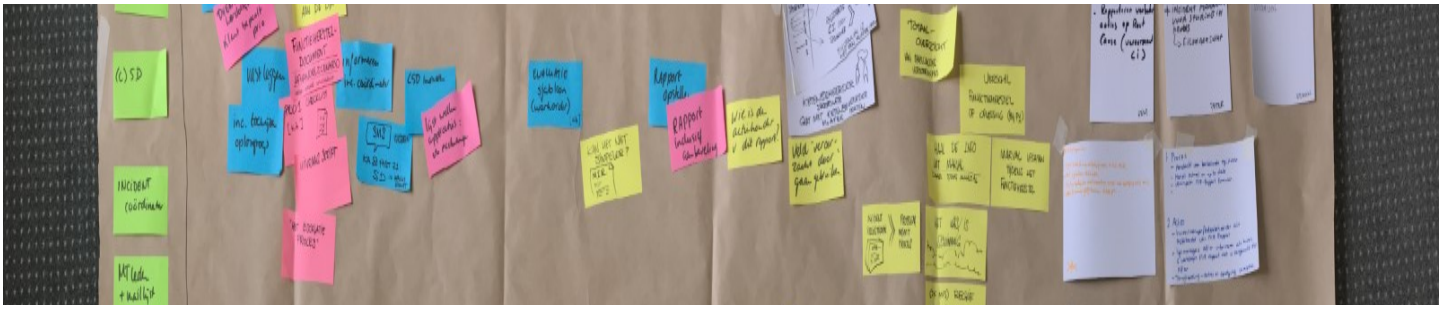


Incidentmanagement



Smans, N.A.J.A. (Nicky)
Procesleider Procesmanagement

Gepubliceerd: 18-3-2022

Het incidentmanagementproces heeft als doel het minimaliseren en verhelpen van nadelige gevolgen voor gebruikers door het zo snel mogelijk herstellen van verstoorde ICT diensten. Dit proces wordt voornamelijk door de Centrale Servicedesk (CSD) van ProRail en de helpdesk van Conclusion (externe leverancier) gebruikt. Dit noemen we de eerstelijns ondersteuning. Andere ICT-afdelingen of externe leveranciers kunnen een tweede- en derdelijns rol hebben. Die rol levert meer specialistische kennis op het gebied van een bepaalde applicatie of keten. Incidenten worden ingedeeld in verschillende prioriteitsklassen; Prio 1, 2 of 3. Dit zegt iets over de urgentie en impact. De oplostijd waarin een incident opgelost moet worden, wordt bepaalt door de prioriteit en het serviceniveau. Een storing met impact op de treindienst moet altijd zo snel mogelijk verholpen worden. Het doel is het tijdig weer verhelpen van de verstoring door middel van een oplossing of een workaround.

Soms is er sprake van een security incident. Dit zijn bewuste aanvallen op de systemen en diensten van ProRail. Een security incident wordt op de gebruikelijke wijze afgehandeld, maar er wordt ook een security officer ingeschakeld. Zie voor meer informatie ICT Information Securitymanagement.
Bij ernstige verstoringen kan een Prio1 incident worden opgeschaald naar een Prio1 calamiteit. Dit houdt in dat de Incident Coördinator gaat opschalen volgens de procedure die staat beschreven in de calamiteitenprocedure.
Het gaat hier met name om complexe Prio1 incidenten met ernstige hinder. Het doel van het opschalen is om met meer menskracht structuur te brengen en zo het incident onder controle krijgen.

Globaal procesverloop

Zodra een gebruiker een storing meldt wordt deze als incident geregistreerd en de prioriteit wordt bepaald. Er wordt gekeken of het incident eerder is voorgekomen en hoe het toen is opgelost. In dat geval is er al een afhandelscenario bekend waardoor het incident snel verholpen kan worden. Is het incident niet eerder opgetreden dan moet worden uitgezocht wat er aan de hand is. Waardoor gebeurt het? De oorzaak wordt onderzocht en er volgt een diagnose. Daarna kan het hersteld worden. Wanneer het incident daadwerkelijk verholpen is, wordt het incident afgesloten.

Rollen en verantwoordelijkheden

Gebaseerd op de hiervoor genoemde leidende principes zijn de verantwoordelijkheden voor de rollen bepaald.

De incidentcoördinator

De incidentcoördinator (IC) is verantwoordelijk voor het bewaken en aansturen Procesgang Incident Management. De IC'er voert de regie bij prio 1 incidenten, draagt zorg voor het tijdig en effectief escaleren conform escalatieprocedures voor incidenten. Verder zorgt hij/zij voor de kwaliteitsborging van incidenten: toezien op correcte (administratieve) afwikkeling van incidenten conform de afspraken. De IC'er is verantwoordelijk voor adequate procedures en levert de input voor de rapportages.

De beheerder eerste lijn, helpdeskmedewerker

De eerstelijns beheerder, meestal de helpdeskmedewerker, registreert de incidenten en blijft eigenaar van het incident gedurende de gehele afhandeling. de helpdeskmedewerker fungeert als single point of contact richting klantorganisatie en ICT Infrastructuur en Operatie. Verder bepaalt hij/zij in overleg met de klant de prioriteit van incidenten (tijdens het proces kan de prioriteit aangepast worden). Ook verzorgt de persoon het matchen/correleren van incidenten, events en problems. Daarnaast maakt de helpdeskmedewerker een risicoanalyse/een oplossing analyse en pleegt functieherstel. Tot slot bewaakt de helpdeskmedewerker de doorlooptijd van incidenten in relatie tot de afspraken welke zijn vastgelegd in de klantafspraken en het nemen van passende maatregelen indien nodig. Hierbij hoort ook het tijdig en effectief escaleren (zowel functioneel als hiërarchisch) conform de geldende procedures.

De beheerder tweede en derde lijn

De tweede- of derde lijn beheerder is de hulplijn voor de eerste lijn-medewerker. Hij maakt de risico/oplossing analyse en ondersteunt/realiseert het functieherstel (op locatie). Ook bewaakt hij/zij de doorlooptijd incidenten in relatie tot de afspraken welke zijn vastgelegd in de klantafspraken en adviseert de eerste lijn in het nemen van passende maatregelen. Daarnaast adviseert hij/zij de eerste lijn in het tijdig en effectief escaleren (zowel functioneel als hiërarchisch) conform de geldende procedures. Verder is hij/zij verantwoordelijk voor adequate werkinstructies zowel procesmatig als technisch. Hij zorgt voor complete, tijdige en correcte registratie van het functieherstel waarvan terugkoppeling vindt aan de eerste lijn.

Extra rollen bij een calamiteit

Indien er sprake is van een calamiteit, dan zullen ook andere rollen worden opgeschaald. Zie voor deze rollen en het moment waarop deze optreden het overzicht in de calamiteitenprocedure.

Toelichting procesfasen

Het globale procesverloop uitgewerkt in fasen

Fase 1 - Registreren en prioriteit bepalen

Door zowel eindgebruikers als vanuit een melding kan een incident geïdentificeerd worden. Na het loggen wordt gecontroleerd of het daadwerkelijk een incident is. Ook wordt bepaald op welke dienst(en) dit incident betrekking heeft. Afhankelijk van de dienst, de urgentie en de impact wordt de prioriteit in overleg met de klant of melder vastgesteld en de bij de prioriteit behorende procedure opgestart. De klant bepaalt de prioriteit.

Bijzonderheden:

- In het geval van een security incident wordt altijd de wachtdienst of een security officer geïnformeerd. Verder wordt dit afgehandeld als een incident.
- In geval van een ernstig incident zoals een complex Prio1 incident met grote impact kan de IC'er in overleg met de Wachtdienst 3 besluiten op te schalen volgens de calamiteitenprocedure.
- In geval van consequenties voor de veiligheid op het spoor moeten er maatregelen genomen worden om deze veiligheidsrisico's te mitigeren. Hiervoor is een procedure beschikbaar.

Het doel is het vastleggen en prioriteren van het incident zodat het op de juiste wijze snel afgehandeld kan worden.

Het resultaat is een geregistreerd en geprioriteerd incident, dat is getoetst en waarbij de volgende zaken zijn vastgelegd: Klant, Dienst, Omschrijving, CI (Configuration item) koppelen, Kantoorautomatisering, Post21 of PIADD(een ander hoog beschikbaar platform) (zit gekoppeld aan dienst).

Dit vastleggen gebeurt allemaal door de helpdeskmedewerker (eerste lijn). De hulpmiddelen hierbij zijn de servicemanagementtool Marval, afhandelscenario's, werkinstructies en functieherstelddocumenten, mail en telefoon.

Fase 2 - Onderzoek en diagnose

Bij de initiële analyse en diagnose wordt getracht om aan de hand van kennisgegevens en known-errors te bepalen of het een bekend probleem betreft. Uit het onderzoek wordt duidelijk of het incident direct op te lossen is of doorgezet moet worden naar de 2e lijn. Er is onderzoek gedaan naar de oorzaak van het incident. Tevens is vastgesteld of er een Known Error geregistreerd is en of er een workaround voor handen is. Ook is er een besluit genomen over het tijdstip waarop het functieherstel gepleegd wordt..

Het doel is om duidelijk te krijgen op welke manier en hoe snel het incident op te lossen is en wie dat moet doen. De oorzaak van het incident is vastgesteld en het herstel kan gaan plaatsvinden. Ook in deze fase is het incident in handen van de eerste lijnmedewerkers, vaak in overleg met een IC'er. Net als in de eerste fase zijn de hulpmiddelen Marval, afhandelscenario's, functieherstelddocumenten, werkinstructies en noodprocedures, mail en telefoon.

Fase 3 - Oplossen, functieherstel

Hier staat het oplossen van het incident centraal (de functie is hersteld). Dit kan gerealiseerd zijn door het doorlopen van een afhandelscenario of het toepassen van een Functieherstel Document. Als het niet mogelijk is een incident direct te herstellen is er mogelijk wel een workaround beschikbaar. Dan wordt de dieperliggende oorzaak later gezocht middels het proces Problem-management. Vaak is er dan een wijziging/change nodig om het incident op te lossen. In geval van een urgent incident kan er direct een wijziging worden uitgevoerd door een zogenaamde spoedchange.
De medewerker van de servicedesk is hier nog steeds in de lead maar heeft

nauw contact met tweede en derde lijn beheerders. Hulpmiddelen zijn Marval, diverse documenten, werkinstructies, mail en telefoon.

Fase 4 - Afsluiten

Het incident is opgelost. De medewerker van de servicedesk zal de oorspronkelijke melder telefonisch informeren. Als het om een incident gaat waar meer mensen hinder van ondervonden kan dit ook via een algemene mail of Focus gaan. Hierna wordt de melding in het servicemanagementsysteem Marval afgesloten. Dit gebeurt met behulp van een afsluitcode.

Wat levert het proces op?

De resultaten van het proces Incidentmanagement zijn:

- *Verholpen incident*
  Het incident is binnen de gestelde responstijd verholpen.
- *Kennis*
  Er is nieuwe kennis opgedaan door dit incident. Dit is vastgelegd in de servicemanagementtool en kan opnieuw gebruikt worden als dit incident zich opnieuw voordoet. Ook kan de kennis leiden tot het aanpassen van een onderdeel of instelling waardoor een dergelijk incident niet meer kan optreden.

Start van het proces

- *Melding van een medewerker of een dienst*
  Er is een medewerker die een (gehele of gedeeltelijke) verstoring van een dienst meldt. De melding kan ook van een systeem komen. Zie hiervoor Eventmanagement
- *Melding vanuit het Nationaal Cyber Security Centrum (NCSC)*
  Het NCSC is permanent bezig met het voorkomen van en reageren op cyberaanvallen. Grote landelijke dreigingen waarbij de continuïteit van ProRail in gevaar kan komen worden 24/7 vanuit het NCSC rechtstreeks en telefonisch gemeld bij de Incident Controllers van de CSD. Zij zorgen dat er een incident wordt geregistreerd en dat deze adequaat word afgehandeld.

Hoe passen (ICT) afdelingen dit proces toe?

Niet alle ICT afdelingen werken op exact dezelfde wijze binnen dit proces. Hier volgen de aandachtspunten.

- Prio 1 incidenten worden altijd geëvalueerd. De template en werkinstructie vind je HIER

- *ICT Infrastructur en Operatie, Helpdesk van Conclusion*
  Zowel Conclusion als de CSD binnen ICT Infrastructuur en Operatie kennen een eigen werkwijze binnen dit proces. Dit zit voor het grootste deel binnen Marval vastgelegd. Daarnaast worden medewerkers ondersteund met procedures en werkinstructies. Deze worden op de eigen teamsites beheerd.

- *ICT afdeling CC ERP*
  De afdeling CC ERP heeft deels een andere werkwijze voor incidenten buiten kantoortijden. Hierover hebben zij afspraken gemaakt met hun leverancier. Kijk hier voor de procedure Incidentmanagement CC ERP.

- *ProRail afdeling AM*
  Met de afdeling Assetmanagement is de onderstaande werkwijze afgestemd. De werkwijze is vastgelegd Procedure afhandeling Cybersecurity Incidenten OBI - CSD

Sturing en rapportage

Procesindicatoren worden ingezet om de kwaliteit van zowel het proces zelf als de resultaten (KPI) uit het proces te kunnen bewaken. De verantwoording voor deze procesindicatoren ligt bij Procesmanagement.

- *TAO-Rapportage*
  Het doel van deze rapportage is het vastleggen en analyseren van het aantal incidenten die een TAO (Treindienst aantastende onregelmatigheid) veroorzaakt hebben. Daarnaast wordt gekeken naar de klanthinder (TVTA, Te Verklaren Trein Afwijking, d.w.z. iedere trein die daarna ook last had van het incident). Deze rapportage wordt gepubliceerd op het Procesdashboard ICT in Power BI.

Incidentmanagement gerelateerde documenten

Onderstaande documenten hebben een directe link met de afhandeling van Prio1 ICT incidenten.

- Calamiteitenprocedure
- Leidraad Wachtdienst 2 / Incident Coördinator (onder constructie)
- Leidraad Wachtdienst 3
- Prio 1 Evaluatie Rapport (P1ER) --> site met blanco en verwerkte rapporten

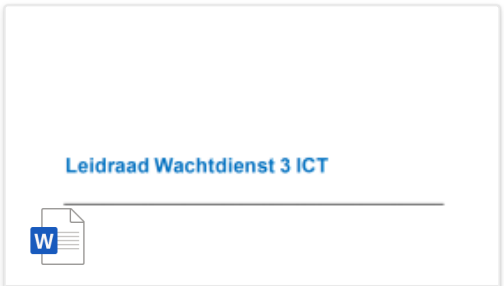
Procesdocumenten



Way of Working ICT

Calamiteitenprocedure 03-21

Rozema, J. (Jurjan)
Heeft 30 maart bewerkt



Way of Working ICT

Leidraad Wachtdienst 3 2021 Q1

Smans, N.A.J.A. (Nicky)
Heeft 24 maart bewerkt



Way of Working ICT

Leidraad Wachtdienst 2 ICérs

Rozema, J. (Jurjan)
Heeft 7 april bewerkt



Way of Working ICT

Maatregelen en communicatie bij onveilige situaties ICT

Hartog, M.I. den (Marieke)
Heeft 16 december 2021 bewe...

Way of Working ICT

P1ERtemplate en verslagen

Hartog, M.I. den (Marieke)
Heeft 26 oktober 2021 bewerkt



Way of Working ICT

Template & werkinstructie 24 uursrapportage versie 1.0

Hartog, M.I. den (Marieke)
Heeft 20 april 2021 bewerkt



Way of Working ICT

Template & werkinstructie Post Mortemrapportage versie 1.0

Hartog, M.I. den (Marieke)
Heeft 20 april 2021 bewerkt



Way of Working ICT

Template Afhandelscenarios Post 21

Hartog, M.I. den (Marieke)
Heeft 26 september 2018 bewe...



Way of Working ICT

Werkinstructie maken Prio 1 Evaluatie Rapport

Hartog, M.I. den (Marieke)
Heeft 20 april 2021 bewerkt

Terug naar boven

Over deze pagina

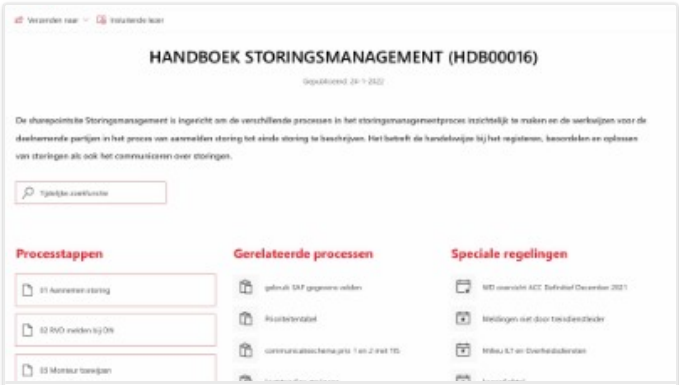
- Eigenaar is procesmanagement

- Wijziging(en) sinds vorige versie
    - Procedure maatregelen en communicatie bij onveilige situaties ICT toegevoegd
    - Layout bijgewerkt

Inhoud

- Globaal procesverloop
- Rollen en verantwoordelijkheden
- Toelichting procesfasen
- Wat levert het proces op?
- Start van het proces
- Hoe passen ICT Afdelingen dit proces toe?
- Sturing en rapportage

Snel naar



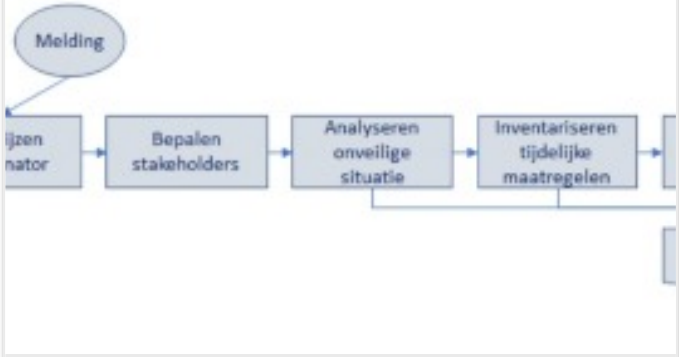
HANDBOEK STORINGSMANAGEMENT (HDB00016)



ICT Information Securitymanagement



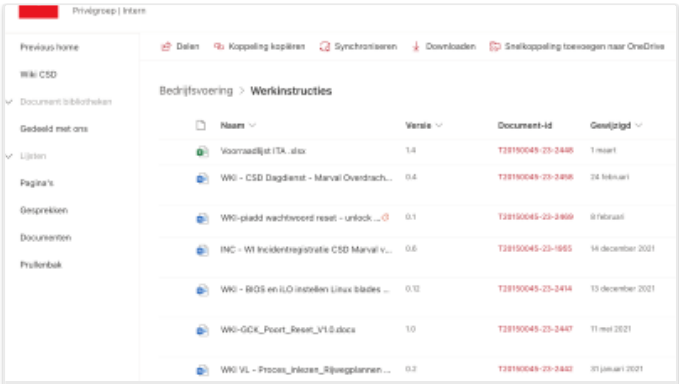
Incidentrapportage



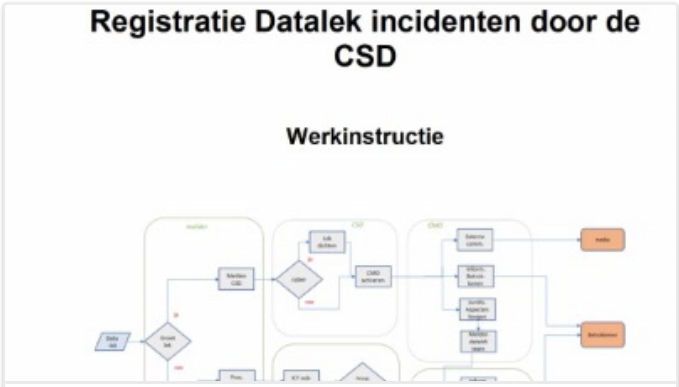
Maatregelen en communicatie bij onveilige situaties ICT



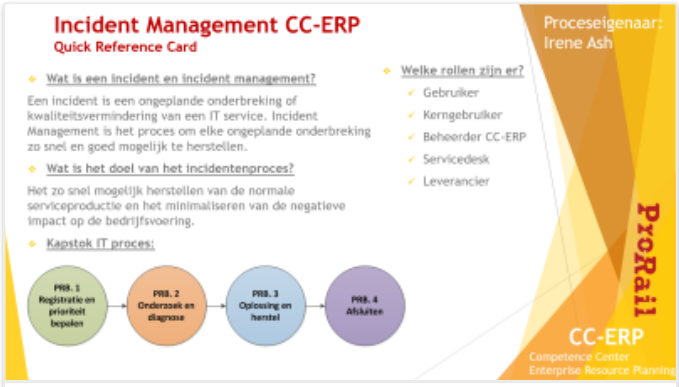
Template Afhandelscenario's Post 21 (document)



Werkinstructies CSD (Sharepoint)

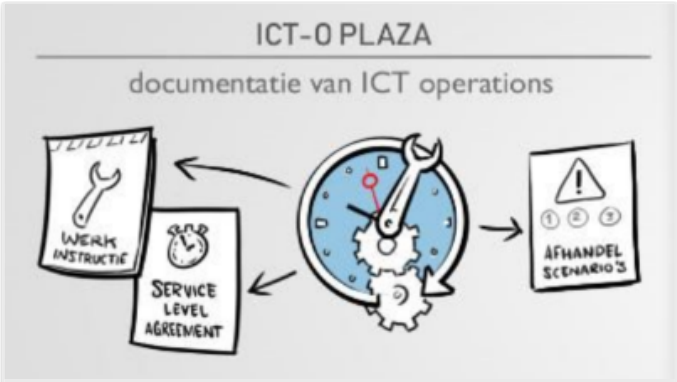


Werkinstructie incidentmanagement Omgang datalekken CSD



Procedure Incident management CC-ERP

Zie ook



ICT-Plaza



Safetymanagementproces