



Bijlage N. Incident Classificatie en Procedure

1. Classificatie van Incidenten

Control Center MKO (hierna CCMKO) van RWS-CIV bepaalt de classificatie van een Incident. Op basis van deze classificatie dient de Opdrachtnemer te acteren conform de onderstaande tabel.

Type Incident	Impact	Urgentie	Business Impact	Service Window	Reactie tijd	Max. TTR
PRIO-1 - Critical	1-High	1-High	Ja	7x24	10 min	60min
PRIO-2 - High	1-High	2-Medium	Ja	kantoor	30 min	240min
	2-Medium	1-High	Ja	kantoor	30 min	240min
PRIO-3 - Moderate	1-High	3-Low	Nee	Kantoor		
	2-Medium	2-Medium	Nee	Kantoor		
	3-Low	1-High	Nee	Kantoor		
PRIO-4 - Low	2-Medium	3-Low	Nee	Kantoor		
	3-Low	2-Medium	Nee	Kantoor		
PRIO-5 - Planning	3-Low	3-Low	Nee	Kantoor		
Security - PRIO-1 - Critical	1-High	1-High	Ja	7x24	10min	30min
Security - PRIO-2 - High	1-High	2-Medium	Ja	kantoor	60min	60min
	2-Medium	1-High	Ja	kantoor	60min	60min
Security - PRIO-3 - Moderate	1-High	3-Low	Nee	Kantoor		
	2-Medium	2-Medium	Nee	Kantoor		
	3-Low	1-High	Nee	Kantoor		
Security - PRIO-4 - Low	2-Medium	3-Low	Nee	Kantoor		
	3-Low	2-Medium	Nee	Kantoor		
Security - PRIO-5 - Planning	3-Low	3-Low	Nee	Kantoor		

2. Major Incidenten

Major Incidenten zijn Incidenten met Business Impact. RWS CIV spreekt van een Major Incident als de door het RWS domein opgestelde criteria geraakt worden. Er is dan sprake van een verstoring die de dienstverlening van het RWS domein zodanig treft, dat de veiligheid en doorstroming in het geding komen of het imago van RWS aantast

De stakeholders binnen CIV worden tijdens een Major Incident door CCMKO ieder uur op de hoogte gehouden van de status. Om dit te kunnen doen is statusinformatie benodigd van de Opdrachtnemer. CCMKO verwacht van de Opdrachtnemer ieder uur een statusupdate. Na afloop van het Major Incident dient de oplospartij een technisch evaluatie rapport op te leveren volgens het beschikbare template. Dit technisch evaluatie rapport moet binnen 5 werkdagen aan km-mko@rws.nl gestuurd worden.

Alleen CCKMO mag een Major Incident uitroepen. Een Major Incident is bij CCMKO altijd een PRIO-1, maar een PRIO-1 is niet altijd een Major Incident.

3. Incident Procedure

Bij de aanmelding van een (Security) Incident dient de Opdrachtnemer in zijn ITSM-tool per (Security) Incident het volgende te registreren:

1. Extern referentienummer wat refereert naar het registratienummer in TOPdesk,
2. Reactietijd,
3. Hersteltijd,
4. Wachtijd,
5. Informatie over actuele status,
6. Status logging.



De Opdrachtnemer dient te reageren op de melding van het (Security) Incident via zijn ITSM-tool en dient bij PRIO-1 en PRIO-2 (Security) Incidenten **terstond** telefonisch contact op te nemen met de melder.

De reactie van de Opdrachtnemer dient minimaal te bestaan uit:

1. statusmelding van de afhandeling van het (Security) Incident;
2. vermelding van de mogelijke oorzaak van het (Security) Incident;
3. vermoedelijk moment van oplossing van het (Security) Incident;
4. afspraak wanneer de volgende statusmelding wordt verwacht.

De Opdrachtnemer dient PRIO-1 (Security) Incidenten met de grootst mogelijke spoed op te lossen via een separaat proces. De Opdrachtnemer dient CCMKO uiterlijk 5 minuten vooraf te informeren bij een dreigende overschrijding van de Max. TTR in de tabel op de vorige pagina.

De Opdrachtnemer dient bij het constateren van een PRIO-1 (Security) Incident CCMKO **terstond** telefonisch te informeren binnen de reactietijd op een vooraf overeengekomen wijze en telefoonnummer.

De Opdrachtnemer dient PRIO-1 en PRIO-2 (Security) Incidenten altijd te registreren in zijn ITSM-tool voordat ze afgehandeld worden.

Wanneer de strategische doelen van RWS geraakt worden omdat een (Security) Incident te lang openstaat, heeft RWS de mogelijkheid om, via een specifieke rol in de RWS organisatie, een PRIO-2 (Security) Incident te promoveren naar een PRIO-1 (Security) Incident. Na deze promotie dient de Opdrachtnemer het (Security) Incident als een PRIO-1 (Security) Incident af te handelen, waarbij de Maximale TTR voor een PRIO-1 (Security) Incident gaat lopen. Naderhand wordt geëvalueerd in hoeverre deze (Security) Incidenten rechtmatig gepromoveerd zijn.

De Opdrachtnemer moet de voortgang en gemaakte afspraken in zijn ITSM-tool bijwerken in voor de Opdrachtgever begrijpelijke taal (dus niet een uitsluitend technische log), waarbij de datum, tijd en het gebruiker-id automatisch dienen te worden toegevoegd.

De Opdrachtnemer dient informatie over instellingen, configuraties, Events en gelogde informatie tijdens (Security) Incidenten te delen met CCMKO, zodat (Security) Incidenten snel herleid kunnen worden naar oorzaak en beheerdomein.

4. Aanvullende procedure bij Security Incidenten

De Opdrachtnemer dient Security Incidenten altijd op te lossen binnen de gestelde Max. TTR tijden.

De Opdrachtnemer dient bij het constateren van PRIO-1 of PRIO-2 Security Incidenten een door de Opdrachtgever tijdens de Project Start Up nader aan te wijzen contactpersoon en/of afdeling telefonisch te informeren binnen de reactietijd. Indien deze contactpersoon en/of afdeling niet bereikbaar is, dient de Opdrachtnemer een voicemail en/of sms en/of whatsapp achter te laten binnen de reactietijd en een email naar deze contactpersoon en/of afdeling te sturen.