

Nummer	Wetstekst/Architectuur/Risico	Eis
#001	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 1. Werkzaamheden Risico gebaseerde aanpak De aanbieder heeft een actueel overzicht van de netwerk- en informatiesystemen die zijn essentiële dienst ondersteunen.	De SOC dienst gebruikt de door Juva aangeleverde assetinformatie, die is voorzien van risico classificatie, bij de beoordeling van detectie en respons. Tevens koppelt de SOC(-dienst) nieuwe assetinformatie en correcties terug naar Juva.
#002a	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 3. Incidenten voorkomen Identificatie- en toegangsmanagement	De SOC(-dienst) monitort toegang en detecteert/rapporteert verdachte inlog(pogingen) qua gedrag en toegang
#002b	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 3. Incidenten voorkomen Identificatie- en toegangsmanagement	De SOC(-dienst) monitort autorisatiewijzigingen en detecteert/rapporteert verdachte autorisatiewijzigingen
#002c	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 3. Incidenten voorkomen Identificatie- en toegangsmanagement	De SOC(-dienst) controleert periodiek op juistheid van de autorisaties en rapporteert dit naar de opdrachtgever
#003	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 3. Incidenten voorkomen Asset-, patch-management	De SOC(-dienst) ondersteunt bij asset- en patch-management door adviezen betreffende updates & patches voor firmware en software. Dit gebaseerd op inzicht in kwetsbaarheden en risicoverhogende afwijkingen.

#004a	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 3. Incidenten voorkomen Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op beveiligingsadviezen en dreigingsinformatie, beoordeelt hij of op basis daarvan gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's te verkleinen naar een passend niveau.	De SOC(-dienst) dient op basis van beveiligingsadviezen en dreigingsinformatie van leveranciers/betrokken overheidsinstanties te beoordelen en vervolgens te rapporteren of aanvullende maatregelen nodig zijn om risico's te verkleinen. SOC(-dienst) kan tevens dreigingsinformatie hiervoor ontvangen voor exclusief gebruik voor N.V. Juva van het Nationaal Detectie Netwerk en een toekomstige EU equivalent.
#004b	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 3. Incidenten voorkomen Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op beveiligingsadviezen en dreigingsinformatie, beoordeelt hij of op basis daarvan gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's te verkleinen naar een passend niveau.	SOC(-dienst) heeft aantoonbaar processen ingericht om adequaat te reageren op dreigingsinformatie vanuit N.V. Juva.
#004c	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 3. Incidenten voorkomen Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op beveiligingsadviezen en dreigingsinformatie, beoordeelt hij of op basis daarvan gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's te verkleinen naar een passend niveau.	SOC(-dienst) kan dreigingsinformatie terugleveren voor exclusief gebruik voor N.V. Juva aan partijen binnen Netbeheer Nederland.

#004d	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 3. Incidenten voorkomen Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op beveiligingsadviezen en dreigingsinformatie, beoordeelt hij of op basis daarvan gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's te verkleinen naar een passend niveau.	SOC(-dienst) kan dreigingsinformatie ontvangen voor exclusief gebruik voor N.V. Juva van partijen binnen Netbeheer Nederland.
#004e	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 3. Incidenten voorkomen Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op beveiligingsadviezen en dreigingsinformatie, beoordeelt hij of op basis daarvan gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's te verkleinen naar een passend niveau.	SOC(-dienst) neemt NCSC beveiligingsadviezen aantoonbaar mee in het beoordelen van de ernst van kwetsbaarheden.
#005a	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 4. Detectie en respons De aanbieder heeft de beveiliging van zijn netwerk- en informatiesystemen zodanig ingericht dat hij daarmee incidenten kan detecteren, analyseren en vastleggen en de gevolgen daarvan zo veel mogelijk kan beperken.	De SOC(-dienst) levert en/of sluit aan op bestaande veiligheidsvoorzieningen voor het detecteren, analyseren en vastleggen van incidenten, en brengt op basis hiervan advies uit om de gevolgen hiervan te beperken. De SOC(-dienst) voorziet in / geeft adviezen voor het verbeteren van de collection capability.

#005b	Bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen, 4. Detectie en respons De aanbieder heeft de beveiliging van zijn netwerk- en informatiesystemen zodanig ingericht dat hij daarmee incidenten kan detecteren, analyseren en vastleggen en de gevolgen daarvan zo veel mogelijk kan beperken.	De SOC(-dienst) voorziet de incidenten, die vastgelegd zijn, van een prioriteit gebaseerd op de risicoclassificatie bij #001. Ook worden patches geprioriteerd.
#006a	Werkzaamheden Detectie en respons 4.2 Hij monitort netwerk- en informatiesystemen structureel op kwetsbaarheden en mogelijke compromittatie en houdt hierbij rekening met de beschikbare dreigingsinformatie	De SOC(-dienst) monitort geselecteerde netwerk- en informatiesystemen op kwetsbaarheden en mogelijke inbreuk en houdt hierbij rekening met de beschikbare algemene + NDN dreigingsinformatie, en stemt deze monitoring af op basis van de belangrijkste dreigingsactoren van NV JUVA
#006b	Werkzaamheden Detectie en respons 4.2 Hij monitort netwerk- en informatiesystemen structureel op kwetsbaarheden en mogelijke compromittatie en houdt hierbij rekening met de beschikbare dreigingsinformatie	Voorziet in security monitoring tools en zorgt dat deze tools up-to-date zijn, dan wel adviseert inzake monitoring tools en het up-to-date houden daarvan.
#006c	Werkzaamheden Detectie en respons 4.2 Hij monitort netwerk- en informatiesystemen structureel op kwetsbaarheden en mogelijke compromittatie en houdt hierbij rekening met de beschikbare dreigingsinformatie	Voorziet in het verzamelen en correleren van log data waarna middels analyse tooling mogelijke security issues in beeld gebracht worden.
#007	Werkzaamheden Detectie en respons 4.3 Hij verzorgt het loggen van de handelingen op de netwerk- en informatiesystemen en bewaart deze gegevens lang genoeg om incidenten te kunnen analyseren	De SOC(-dienst) monitort de logging van de handelingen op de netwerk- en informatiesystemen lang genoeg om incidenten te kunnen analyseren. De duur van de bewaartermijn wordt in onderling overleg bepaald a.d.h.v. security practises.
#008a	Werkzaamheden Detectie en respons 4.4 Hij hanteert procedures omtrent het optreden bij incidenten.	Op informatiebeveiligingsincidenten behoort te worden gereageerd middels standaard procedures die in overeenstemming zijn met de betreffende procedures van Juva.

#008b	Werkzaamheden Detectie en respons 4.4 Hij hanteert procedures omtrent het optreden bij incidenten.	De SOC(-dienst) verbetert eigen processen en adviseert over het verbeteren van de beveiliging bij N.V. Juva naar aanleiding van een incident.
#008c	Werkzaamheden Detectie en respons 4.4 Hij hanteert procedures omtrent het optreden bij incidenten.	Er behoort een categoriserings- en prioriteringsschema voor informatiebeveiligingsincidenten te worden overeengekomen voor het identificeren van de gevolgen en prioriteit van een incident. Het schema behoort de criteria te omvatten voor het als informatiebeveiligingsincident categoriseren van gebeurtenissen. Het contactpunt behoort elke informatiebeveiligingsgebeurtenis aan de hand van het overeengekomen schema te beoordelen.
#013a	Werkzaamheden Gevolgen van incidenten beperken 5.2 Het crisismanagementbeleid bestaat in ieder geval uit een plan om de essentiële dienst zo spoedig mogelijk te herstellen na een incident.	De SOC(-dienst) ondersteunt Juva bij het oplossen van security incidenten en draagt bij aan eventueel herstel na schade vanwege security incidenten. Voor dit laatste is het herstelplan van Juva leidend maar niet beperkend.
#013b	Werkzaamheden Gevolgen van incidenten beperken 5.2 Het crisismanagementbeleid bestaat in ieder geval uit een plan om de essentiële dienst zo spoedig mogelijk te herstellen na een incident.	Documenteert reacties naar aanleiding van incidenten en oplos- en herstelacties. Gaat na of incidenten volledig zijn verholpen, zodat deze incidenten niet meer voor kunnen komen.
#014	Werkzaamheden Gevolgen van incidenten beperken 5.3 Het crisismanagementbeleid wordt daartoe periodiek in de praktijk beoefend.	Neemt deel aan crisismanagement- en cyberoefeningen.
#015	Architectuur uitgangspunt	Wanneer netwerk- en informatiesystemen in eilandbedrijf opereren kan de SOC(-dienst) de detectie en respons capabilities die het bezit onverminderd voortzetten. Hiertoe kan het benodigd zijn dat de SOC dienst fysiek in dienstverlening op locatie moet kunnen voorzien.
#016	AVG	SOC-dienst sluit een geheimhoudingsovereenkomst en een verwerkersovereenkomst af met N.V. Juva en legt verplichtingen voortvloeiend uit deze overeenkomsten aantoonbaar op aan alle relevante leveranciers.

#017	Werkzaamheden Detectie en respons 4.4 Hij hanteert procedures omtrent het optreden bij incidenten.	SOC(-dienst) bewaakt het doel en monitort de effectiviteit van nieuwe en bestaanden use cases.
#018		SOC-dienst is ISO27001 gecertificeerd.
#019		Data van N.V. Juva wordt alleen binnen de EER verwerkt.
#020		SOC dienst monitort toegang tot het netwerk en de wijzigingen die worden aangebracht door gebruikers.
		EDU: hebben wij nog technische/security eisen hoe een SOC gekoppeld wordt aan ons OT domein voor actuele inzichten en in welke systemen het SOC zou moeten kunnen/mogen om bv te verifiëren of mitigeren?
#021	Juva/WI algemeen-security	Juva/Westland Infra volgt ENCS: https://encs.eu/resources/ . Voor wat betreft Security. Het SOC moet voldoen aan de door het ECNS gestelde eisen en randvoorwaarden passend bij een secure Hardware en Netwerk opzet te voorzien door Westland Infra.
#022	Juva/WI algemeen-security	Met name "SC-301-2020: Security requirements for procuring SCADA applications" vormt de basis voor de door Westland Infra voor OT beoogde security voorzieningen. Hieraan moet volledig in voorzien worden, dit wel in combinatie met hardware, software en netwerk.