

Bijlage 09 - Beveiligingsnormen Nuffic 2017

Hoofdonderwerp	Korte Code	Onderwerp	Normen	Baseline beveiligd	Additioneel beveiligd	Scope beveiliging	Software as a Service			Opmerking / Specificatie
							Platform as A Service			
							hosting en IAAS	Technisch beheer	Applicatie beheer	
Geheimhouding		geheimhouding	Geheimhouding wordt in de arbeidsovereenkomst of overeenkomst met dienstverlener overeengekomen, en zo niet wordt een geheimhoudingsverklaring ondertekend	x	x	intern, extern	x	x	x	
Privacy en toegang tot data	CC-OUTS-19	garantie vertrouwelijkheid	De dienstverlener garandeert dat zij de vertrouwelijkheid van Nuffic data beschermt	x	x	extern	x	x	x	Vertrouwelijkheidsclausules: de dienstverlener zal geen klantdata opzoeken, analyseren of opslaan als dit niet nodig is voor technische doeleinden of om fraude of aanvallen op het netwerk van de dienstverlener te bestrijden. Klantdata worden op verzoek van de klant vernietigd. Beleid omtrent het scheiden van klantdata zal worden gecommuniceerd en aan audits onderworpen.
Privacy en toegang tot data	EP-OUTS-02	privacy wetgeving	De informatie van Nuffic moet conform de Privacy wetgeving worden opgeslagen en behandeld.	x	x	intern, extern	x	x	x	
Privacy en toegang tot data	EP-OUTS-04	gegevens binnen EU	Gegevens in rust of in bewerking (incl. backups) blijven binnen EU grenzen	x	x	extern	x	x	x	In situaties waarin de data van een deel van het netwerk van de clouders wordt verplaatst naar een ander deel, zal rekening worden gehouden met welke overheden en jurisdicties aanspraak kunnen maken op de data van een klant.
Privacy en toegang tot data	CC-OUTS-21	procedure voor dataretentie	Dienstverlener verwijdert op verzoek van Nuffic data van Nuffic op veilige wijze in geval van opzegging van het product, na de verplichte bewaarperiode en geeft een verklaring af dat de gegevens zijn vernietigd.	x	x	extern	x	x	x	Het verwijderen van services omvat het volledig vernietigen van alle relevante data, voorafgegaan door een periode van dataretentie.
Privacy en toegang tot data		vernietiging gegevens	Voordat apparatuur en media worden afgevoerd dienen de opgeslagen gegevens te worden verwijderd op niet meer te recoveren wijze.		x	intern, extern	x	x	x	
Dienstverlener		dienstverlener reputatie	De dienstverlener heeft een geldige certificering van ISAE3402 of ISO27001 en deze worden jaarlijks extern geaudit.	x		extern	x	x	x	
Dienstverlener	EP-OUTS-03	dienstverlener reputatie	De dienstverlener heeft een geldige certificering van ISO27001. Voor een financieel systeem is daarnaast een geldige certificering van ISAE3402 vereist. Certificeringen worden jaarlijks extern geaudit.		x	extern	x	x	x	
Meerdere afnemers	CC-MULTI-01	dienstverlener capaciteitsmanagement	Er is genoeg infrastructurele en personele capaciteit beschikbaar, rekening houdend met pieken in gebruik en multi-tenancy. Dit wordt getoetst aan de hand van contractuele afspraken over beschikbaarheid en kennisborging.	x	x	extern	x	x	x	

Meerdere afnemers	CC-MULTI-03	risico van het falen van isolatie	Het risico van het falen van de isolatie in de virtualisatielaag en de storage wordt regelmatig beoordeeld en wordt tot een minimum beperkt	x	x	extern	x	x		Aanvallen op de virtuele infrastructuur (Shimming, Blue Pill, Hyper jacking, etc.) zullen worden geïdentificeerd en tegengegaan met technische en procedurele controlemaatregelen. Regelmaat bepaald ogv risico analyse.
Meerdere afnemers	CC-MULTI-04	afscheiding van netwerk	Omgeving van Nuffic is afgeschermd op het netwerk van andere klanten		x	extern	x	x		Sniffing en ip spoofing worden uitgesloten.
Meerdere afnemers	CC-MULTI-05	controle over hardware bij een dagvaarding	In het geval van een dagvaarding verzet dienstverlener zich binnen de grenzen van de wet, tegen inbeslagname van hardware en data van Nuffic		x	extern	x	x	x	Procedures zijn aanwezig om bij dagvaarding klantdata veilig te extraheren.
Management informatie en controle	CC-OUTS-03	verzetbaarheid van diensten	Nuffic data is overdraagbaar in een vorm die industrie-standaard is. Migraties naar andere dienstverleners worden niet gehinderd.	x	x	extern	x	x	x	
Management informatie en controle	CC-OUTS-04	risicobeoordeling door klant	De dienstverlener zal vooraf informatie verstrekken over het risico op inbeslagname, terminatie van de provider, lock-in risico en verandering in eigendom van de dienstverlener.	x	x	extern	x	x	x	
Management informatie en controle	CC-OUTS-06	ontbreken van toegezegde beschikbaarheid	De dienstverlener komt afspraken die binnen de beïnvloedingsfeer van de dienstverlener vallen na. Onbeschikbaarheid van belangrijke onderdelen van de dienst betekenen ook dat deze niet beschikbaar is. Aangekondigd onderhoud wordt niet als onbeschikbaar gerekend.	x	x	extern	x	x		
Management informatie en controle	CC-OUTS-07	Informatie over resultaten van audits en mitigatie van resultaten die onvoldoende zijn.	De dienstverlener informeert Nuffic over haar auditbeleid, controlemaatregelen en auditresultaten. De dienstverlener informeert Nuffic als de dienstverlener niet voldoet aan de afgesproken standaarden. De dienstverlener krijgt een redelijke periode om weer aan de standaard te voldoen.	x	x	extern	x	x	x	
Management informatie en controle	CC-OUTS-08	extreme verzoeken met betrekking tot oplevering	De dienstverlener informeert Nuffic als zij een extreem bestelpatroon in het account van Nuffic constateert. Nuffic moet een harde limiet aan de maximale kosten kunnen instellen.	x	x	extern	x	x	x	
Management informatie en controle	CC-OUTS-09	het staken van de activiteiten van de dienstverlener	Indien de dienstverlener onverwachts zijn activiteiten staakt, krijgt Nuffic toegang tot data en eigendommen.	x	x	extern	x	x	x	
Management informatie en controle	CC-OUTS-09a	het staken van de activiteiten van de dienstverlener	Dienstverlener werkt mee aan Escrow overeenkomst indien zij het intellectueel eigendom heeft over maatwerk voor Nuffic. De volledige broncode wordt dan per major release bijgewerkt en met een afgesproken frequentie gedeponneerd bij een derde.	x	x	extern	x	x	x	
Management informatie en controle	CC-OUTS-10	het opzeggen van diensten door de dienstverlener	De dienstverlener zegt het contract met Nuffic alleen op korte termijn op als de wet haar daartoe dwingt, als Nuffic de diensten niet betaalt of als overtredingen van de fair use policy worden genegeerd. De dienstverlener waarschuwt Nuffic tevoren .	x	x	extern	x	x	x	

Management informatie en controle	CC-OUTS-11	onderbreken van diensten door de dienstverlener	De dienstverlener mag de dienst van Nuffic alleen onderbreken als het door de wet vereist wordt, als Nuffic niet betaalt of als overtredingen van de fair use policy worden genegeerd of de diensten van andere klanten worden bedreigd. Nuffic wordt van tevoren gewaarschuwd indien mogelijk en de dienst zal zo snel mogelijk weer beschikbaar worden gemaakt.	x	x	extern	x	x	x	
Juridisch Proces	CC-OUTS-13	verzamen van bewijsmateriaal voor onderzoeken door klanten	Er is een procedure voor het verzamelen van bewijsmateriaal voor onderzoeken door klanten en informatie over deze procedure is beschikbaar. Geautomatiseerde verzameling van bewijsmateriaal is geïmplementeerd.	x	x	extern	x	x	x	Bewijsbare traceerbaarheid van virtueel bezit (ISO27017): migraties van virtuele machines worden gelogd en beveiligd.
Juridisch Proces	CC-OUTS-14	ondersteunen van onderzoeken door klanten	De dienstverlener werkt mee aan elk redelijk incidentonderzoek door Nuffic, ook door het beschikbaar maken van de relevante logs (dit alles onderhevig aan privacy verplichtingen).	x	x	extern	x	x	x	
Juridisch Proces	CC-OUTS-16	melding van relevante wetgeving en toezichthouders	De dienstverlener informeert Nuffic over wetgeving die relevant is voor de dienstverlening en geeft aan Nuffic gegevens van relevante toezichthouders en rechtbanken door.	x	x	extern	x	x	x	Het communiceren van de relevante wetgeving houdt ook in dat de provider melding zal maken van relevante records waarvan de provider verplicht is die te bewaren. De dienstverlener zal bevestigen of cryptografische technologieën in overeenstemming zijn met de lokale wetgeving (ISO27017).
Juridisch Proces	CC-OUTS-17	gegarandeerd eigendom van data	Nuffic is eigenaar van data. De dienstverlener zal het intellectueel eigendom van Nuffic respecteren.	x	x	extern	x	x	x	
Juridisch Proces	CC-OUTS-18	juridische vertegenwoordiging van de klant	Indien er een juridisch onderzoek komt jegens de diensten die aan Nuffic geleverd worden informeert de dienstverlener Nuffic onmiddellijk.	x	x	extern	x	x	x	
Toegangsbeheer	CC-OUTS-20	toegang van personeel van de dienstverlener tot de omgeving	De dienstverlener stelt op verzoek toegangsrechten van haar personeel en operator logs gerelateerd aan Nuffic omgevingen beschikbaar. In productie omgevingen heeft de dienstverlener alleen de noodzakelijke toegangsrechten voor het beheer.	x	x	extern	x	x	x	
Toegangsbeheer		wachtwoorden	Indien een wachtwoord niet in de AD is opgenomen - omdat dit onmogelijk is - dient deze als volgt beveiligd te zijn: Er wordt gebruik gemaakt van een per user salt van 64 bits of meer. Er wordt gebruik gemaakt van hashing met het bcrypt algoritme.	x	x	extern	x	x	x	
Toegangsbeheer		wachtwoorden	Indien Azure AD wordt gebruikt voor authenticatie mogen er geen gegevens worden opgeslagen uit Azure AD tenzij overeengekomen met IT.	x	x	extern	x	x	x	
Intrastructuur ontwerp	CC-OUTS-22	informatie over beschikbaarheid en performance	De verwachte capaciteit, de mate van redundantie en verwachte hersteltijden op het niveau van de verwerkingslaag, de data-opslag, het interne netwerk en de transit-verbindingen zijn beschikbaar. Dienstverlener neemt maatregelen tegen dataverlies en beschikt over informatie over datacenterlocaties, security, de mate van redundantie en herstelprocedures.	x	x	extern	x	x	x	

Infrastructuur ontwerp	CC-OUTS-23	informatie over beschikbaarheidsverhogende maatregelen	Plannen met betrekking tot disaster recovery en andere beschikbaarheidsverhogende maatregelen worden met Nuffic gedeeld wanneer dit relevant is.	x	x	extern	x	x	x	
Infrastructuur ontwerp	CC-OUTS-24	veranderingen in technologie en change management/wijzigingen beheer	De dienstverlener informeert Nuffic over belangrijke versie upgrades. De dienstverlener houdt bestaande technologieën die Nuffic gebruikt beschikbaar. Wanneer zulke technologie wordt uitgefaseerd, zal dit met een overgangsperiode gebeuren.	x	x	extern	x	x	x	
Infrastructuur ontwerp	CC-OUTS-25	informatie over de beveiligingsstatus en veranderen in beveiligingsprocedures	De dienstverlener informeert Nuffic over veranderingen in beveiligingsprocedures, substantiële wijzigingen in het beveiligingsbeleid, beveiligingsstatus en beveiligingsvereisten.	x	x	extern	x	x	x	
Beveiligingsproces	CC-OUTS-26	audits van zwakke plekken in de beveiliging	Periodiek worden zwakke plekken in de beveiliging en getroffen maatregelen geaudit. De resultaten van deze audits worden gedeeld met Nuffic. Auditrapporten bevatten geen informatie die tot een beveiligingslek kunnen leiden.	x	x	extern	x	x	x	Details met betrekking tot de ISO27017 audit: utiliteitsprogramma's die controlemaatregelen kunnen overschrijven en de maatregelen die deze kunnen beheersen zullen worden geaudit. Maatregelen tegen malware zullen aan een audit worden onderworpen.
Beveiligingsproces	CC-OUTS-27	conflicterende rollen	De dienstverlener past functiescheiding toe in systemen voor eigen processen en processen van Nuffic, voorkomt conflicterende rollen, betreft deze bij het auditproces en informeert Nuffic daarover.	x	x	extern	x	x	x	
Beveiligingsproces	CC-OUTS-28	klantverantwoordelijkheid bij security incidenten	Dienstverlener informeert Nuffic over incidentmanagement en beschikt over een procedure voor klantinput	x	x	extern	x	x	x	
Beveiligingsproces	CC-OUTS-29	beveiligingsonderzoeken door klanten	Op aanvraag van Nuffic zal de dienstverlener een kwetsbaarheden scan (laten) doen.	x	x	extern	x	x	x	
Beveiligingsproces	CC-OUTS-30	informatie over security incidenten	Security incidenten en inbreuken op de privacy worden zo spoedig mogelijk en tenminste op de dag van ontdekking aan de Security Manager van Nuffic gemeld en aan contactpersoon van dienstverlener gemeld en bij diens afwezigheid aan de opdrachtgever van de dienstverlener. Op verzoek van Nuffic worden relevante logs beschikbaar gesteld.	x	x	extern	x	x	x	
Operationeel proces	CC-OUTS-32	informatie en planning aangaande onderhoud en storingen	Dienstverlener informeert Nuffic tijdig over onderhoud en storingen. Onderhoud wordt ingepland zodat de overlast voor Nuffic wordt geminimaliseerd.	x	x	extern	x	x	x	
Operationeel proces	CC-OUTS-33	informatie over verminderde dienstverlening	Bij storingen of verminderde beschikbaarheid van een dienst rapporteert de dienstverlener schriftelijk over de reden en maatregelen.	x	x	extern	x	x	x	
Operationeel proces	CC-OUTS-34	gebruikershandleidingen	De dienstverlener geeft uitleg of een handleiding beschikbaar over de afgenomen diensten.	x	x	extern	x	x	x	Informatie opgenomen in ISO27017: de relevante gebruikte encryptie en informatie over mobiele interactie met de dienstverlener.

Operationeel proces	CC-OUTS-35	beveiliging van de management interface	Publiekelijk beschikbare web applicaties en API's gerelateerd aan de dienst zijn beveiligd. Verbindingen worden gemaakt op basis van sterke wachtwoorden (zie hiervoor) en versleutelde verbindingen.	x	x	extern	x	x	x	Beveiliging houdt ook in: publiek toegankelijke webapplicaties zijn beschermd met IDS en een firewall op applicatieniveau. Tegen kwetsbaarheden in de logica van de applicatie zijn maatregelen genomen: er wordt alleen gebruik gemaakt van queries met vastgestelde parameters, commentaar in code wordt geminimaliseerd, het gebruik van cookies is beveiligd en herziening van code en black box scans worden geregeld uitgevoerd. Ongebruikte publiek toegankelijke functionaliteit wordt verwijderd.
Operationeel proces		configuratie webser	Er wordt standaard via sslabs.com een controle gedaan op de configuratie van de webserver. Er dient tenminste een B beoordeling te worden gehaald.	x		extern	x	x	x	FB/Projectleider checkt zelf of laat dienstverlener checken
Operationeel proces		configuratie webser	Er wordt standaard via sslabs.com een controle gedaan op de configuratie van de webserver. Er dient tenminste een A beoordeling te worden gehaald.		x	extern	x	x	x	FB/Projectleider checkt zelf of laat dienstverlener checken
Operationeel proces		mail	Het verzenden van mail voor alle domeinen dient altijd via Office 365 te gebeuren. Enkel Mailplus mag via zijn eigen servers verzenden.	x	x	extern	x	x	x	
Operationeel proces		mail	E-mail is versleuteld en wordt gescand op virussen.		x		x	x	x	
Interfacen met de dienst	CC-OUTS-36	versleuteling data	Gevoelige data wordt versleuteld opgeslagen. Ongeautoriseerde toegang en opslag van onversleutelde gevoelige financiële informatie is niet mogelijk.	x	x	extern	x	x	x	Gevoelige data houdt onder andere in: Tracks, magnetische stripe data, PIN, PAN, CCV, credit card-nummers.
Interfacen met de dienst		versleuteling data	Vertrouwelijke gegevens mogen enkel verzonden worden door ze tijdens de gehele transportketen over het internet te beveiligen met een actueel versleuteling algoritme. Voor webverkeer is dit HTTPS (certificaat, TLS, minimale CSR sleutellengte van 2048 bits). Verzenden van vertrouwelijke gegevens via e-mail is niet toegestaan.		x	extern	x	x	x	
Interfacen met de dienst		versleuteling data	Van een extern opgeslagen database dienen de actuele keys en andere ontsleutelingsinformatie beschikbaar te worden gesteld aan de Security manager.	x	x	extern	x	x	x	
Interfacen met de dienst		Selfsigned certificaten	Het gebruik van selfsigned certificaten voor communicatie met derden is niet toegestaan. Dit geldt ook voor signed documenten.	nvt		extern	x	x	x	

Interfacen met de dienst	CC-OUTS-37	management interface toegang	Management interfaces van Nuffic staan alleen individuele toegang toe, op basis van autorisatiematrix. Nuffic kan toegangsrechten voor deze management interface eenvoudig wijzigen.	x	x	extern	x	x	x	Informatie over de toegangsprocedures met betrekking tot de management interface zal worden verstrekt, zodat de klant zijn eigen beleid kan ontwikkelen. Toelichting op Management Interface bij: 1) Overige hosting zoals bijvoorbeeld Survey monkey. Niet de applicatie zelf, maar het beheer zoals import gebruikers, aanmaken vragen, backup en restore etc. 2) SaaS - Gebruikers opvoeren, koppelingen met derden opvoeren instellingen van configuratie,, 3) PaaS - Backup beheeren, koppelingen met internet databases of infrastructuur aanmaken 4) IaaS - De interface van de beheertools ESXi, VDI of SSH, ILO in plaats van de toegang of gebruik van de toepassing zelf.
Interfacen met de dienst	CC-OUTS-37a	management interface toegang	Na contractbeëindiging worden onmiddellijk toegangsrechten verminderd. De toegangsrechten van een medewerker worden verminderd als deze anders of geen gebruik meer maakt van de dienst. Informatie over het gebruik van toegangsrechten door medewerkers van Nuffic wordt op aanvraag beschikbaar gemaakt. Extra checks zijn beschikbaar zijn in het geval van acties die data vernietigen.	x	x	extern	x	x	x	Informatie over de toegangsprocedures met betrekking tot de management interface zal worden verstrekt, zodat de klant zijn eigen beleid kan ontwikkelen.
Interfacen met de dienst	CC-OUTS-38	beschikbaarheid van de management interface	De management interface dient altijd beschikbaar te zijn.	x	x	extern	x	x	x	Verdere specificatie: de management interface is onafhankelijk van een enkele fysieke locatie.
Interfacen met de dienst	CC-OUTS-39	autorisatie van klantpersoneel	Verzoeken van medewerkers van Nuffic worden alleen uitgevoerd als die persoon geautoriseerd is volgens het dan gedefinieerde autorisatieniveau (autorisatiematrix).	x	x	extern	x	x	x	