Bijlage 17 Informatiebeveiligingseisen bij inkoop

Inleiding
Binnen Nuffic worden applicaties gebruikt om de bedrijfsprocessen te ondersteunen. Voor de borging van de informatieveiligheid en privacyaspecten van deze applicaties evenals de compliancy verplichtingen van Nuffic zijn informatiebeveiligingseisen vastgesteld die gehanteerd kunnen worden als uitgangspunt voor de inkoop, ontwikkeling en het beheer van deze applicaties.

Doel en toepassingsgebied
Dit document beschrijft de generieke en vastgestelde informatiebeveiligingseisen van Nuffic voor het inkopen, ontwikkelen en beheren van applicaties.

Deze zijn van toepassing op alle applicaties en informatiesystemen die ingezet worden binnen Nuffic en opgesteld voor alle medewerkers die betrokken zijn bij inkoop, ontwikkeling en/of beheer ervan. De eisen zijn tevens van toepassing op de uitbesteding van ontwikkeling en beheer en vormt input voor aanbestedingen hieromtrent.

Scope
Deze eisen zijn opgesteld op basis van de minimaal noodzakelijke aspecten van informatiebeveiliging binnen Nuffic en het minimale beveiligingsniveau dat Nuffic is opgelegd door de compliance verplichting aan wet- en regelgeving zoals de AVG en de BIO.

Additionele eisen
De eisen uit dit document zijn te allen tijde van toepassing (de zogenaamde Nuffic baseline) op alle inkoop- en ontwikkelingstrajecten. Voorafgaand aan een dergelijk traject dient een risicoanalyse uitgevoerd te worden met de Information Security Officer en/of Privacy Officer en kunnen er additionele specifieke eisen worden toegevoegd.

Veilig & betrouwbaar personeel	1	Alle medewerkers ondertekenen een geheimhoudingsverklaring. Alle ingehuurde medewerkers die toegang krijgen of in aanraking kunnen komen tot informatie van Nuffic dienen een positieve Verklaring Omtrent Gedrag te hebben ontvangen (en aangeleverd aan Nuffic). Dienstverleners ondertekenden een geheimhoudingsverklaring en/of zijn contractueel gebonden aan een geheimhoudingsbepaling.
Beheer van bedrijfsmiddelen	2	Informatiesystemen waarop Nuffic informatie is of was opgeslagen dienen op zorgvuldige wijze te worden geschoond van rest data volgens algemeen gebruikelijke standaarden voor datavernietiging (Secure Erase). Minimaal dient de data twee keer overschreven te worden met vaste data, één keer met random data en er dient daarna geverifieerd te worden of de overschrijving gelukt is. Gegevens(dragers) worden vernietigd zodra het niet meer noodzakelijk is gegevens voor een gerechtvaardigd doeleinde te bewaren.
Toegangsbeveiliging	3	Alle accounts waarmee toegang tot systemen van Nuffic of systemen met data van Nuffic via het internet dienen voorzien te zijn van twee-factor authenticatie. Onder gebruikers wordt binnen deze norm verstaan: Nuffic medewerkers, ingehuurde medewerkers, medewerkers van partijen waarmee Nuffic samenwerkt, medewerkers van leveranciers. Indien de applicatie meer dan 10 gebruikers kent is aansluiten op de AzureAD van Nuffic (en gebruik van Single Sign On) verplicht. Alle beheerder- en andere accounts met verhoogde privileges van systemen met toegang tot Nuffic data dienen altijd voorzien te zijn van twee-factor authenticatie.
Toegangsbeveiliging	4	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen via de Nuffic Single Sign on oplossing. Indien deze niet wordt gebruikt dienen onderstaande eisen ingevuld te worden m.b.t. wachtwoorden - minimaal 8 tekens - levensduur van maximaal 90 dagen - de twintig laatst gebruikte wachtwoorden mogen niet worden hergebruikt - het wachtwoord dient tekens te bevatten uit minimaal drie van de onderstaande categorieën: hoofletters, kleine letters, cijfers, symbolen, unicode tekens, gebruikersnaam mag geen onderdeel zijn van het wachtwoord. - het aantal mislukte aanmeldpogingen voordat een account geblokkeerd wordt is 3 Deze eis is van toepassing op gebruikers zoals gedefinieerd in norm 9.4.2 en voor alle klantgroepen.

Cryptografie	5	Er dient versleuteling voor authenticatie, van data transport en opslag te worden toegepast. Er mogen enkel cryptografische technieken worden gebruikt die algemeen als veilig zijn beschouwd. Nuffic hanteert hierbij de adviezen van het NCSC-NL als standaard. Webapplicaties mogen geen http only, SSL2.0, SSL3.0 en/of TLS 1.0 verkeer toe te staan. Webapplicaties dienen wel TLS 1.2 connecties of hoger toe te staan. Certificaten dienen als veilig te worden beschouwd door de bekende browsers (Edge, Firefox, Chrome, Safari). Webapplicaties dienen een score van A of A+ te halen bij de ssllabs.com SSL server test. Het gebruik van selfsigned certificaten voor communicatie met derden, en voor digitaal ondertekenen van documenten is niet toegestaan.
Fysieke beveiliging en beveiliging van de omgeving	6	Fysieke toegang tot systemen en/of data wordt enkel verstrekt aan geautoriseerde personen die de juiste screening hebben doorlopen en individueel of via een bedrijfsovereenkomst de geheimhoudingsverklaring hebben ondertekend.
Fysieke beveiliging en beveiliging van de omgeving	7	Werkplekken die toegang hebben tot Nuffic informatiesystemen of data dienen na een periode van inactiviteit van minimaal 15 minuten automatisch vergrendeld te worden.
Beveiliging bedrijfsvoering	8	De opdrachtnemer neemt in alle redelijkheid maatregelen om de beschikbaarheid van data te garanderen. Gegevens in rust of in bewerking (incl. backups) dienen altijd binnen EU grenzen te blijven.
Beveiliging bedrijfsvoering	9	Er dienen versleutelde back-ups te zijn op een externe locatie. Het verzenden van deze data dient via afdoende versleutelde kanalen plaats te vinden
Beveiliging bedrijfsvoering	10	Logging van alle toegang (inclusief verwijderen en aanpassen) van de data en systemen die worden gebruikt bij het voldoen van dit contract dient beschikbaar te zijn in een bij Nuffic bekende locatie of aangeleverd te kunnen worden (na goedkeuring) voor een periode van minimaal 3 maanden.
Beveiliging bedrijfsvoering	11	Logfiles bevatten minimaal de gebeurtenis, het van en naar IP-adres, waar mogelijk gebruikersnamen, datum, tijd en ondernomen acties.
Beveiliging bedrijfsvoering	12	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld

Beveiliging bedrijfsvoering		
	13	Beheersrechten geformaliseerd zowel technisch als wijzigingsprocedures aanwezig
Beveiliging bedrijfsvoering	14	Er dient een procedure opgesteld, afgestemd en geïmplementeerd te zijn waarin: - ontdekte kwetsbaarheden aan Nuffic worden gemeld; - overleg plaatsvindt over mogelijkheden voor tussentijdse mitigerende maatregelen - patching in geval van ernstige kwetsbaarheden (waarbij Nuffic de NCSC.NL classificatie en adviezen volgt) binnen een week plaatsvindt. In alle andere gevallen dient patching plaats te vinden binnen de reguliere termijn uit de overeenkomst.
Communicatiebeveiliging	15	Email mag niet gebruikt worden voor het verzenden van gevoelige/bijzondere of grote hoeveelheden data. Het verzenden van e-mail dient te versturen via de Exchange omgeving van Nuffic.
Acquisitie, ontwikkeling en onderhoud van informatiesystemen	16	Er dienen aantoonbaar formele procedures te worden gehanteerd waarmee wijzingen aan systemen worden doorgevoerd en beheerst. Wijzigingen op de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Er wordt op een van de productieomgeving gescheiden (acceptatie)test- en ontwikkelomgeving (OTAP) ontwikkeld en getest. Het is niet toegestaan in de productieomgeving te testen.
Acquisitie, ontwikkeling en onderhoud van informatiesystemen	17	Voor het testen van informatiesystemen met persoonsgegevens en voor trainingen voor informatiesystemen worden uitsluitend niet tot personen herleidbare gegevens gebruikt
Leveranciersrelaties	18	Opdrachtnemer moet kunnen aantonen dat zij minimaal voldoen aan ISO 27001/2. Dit kan aangetoond worden middels certificering of een ISAE 3000 (of vergelijkbare) verklaring. Indien de opdrachtnemer geen certificaat kan aantonen dan dient opdrachtnemer middels andere documentatie kunnen aantonen dat de geïmplementeerde maatregelen minimaal conform ISO 27001/2 zijn.

Leveranciersrelaties	19	Met opdrachtnemers die als verwerker voor of namens Nuffic persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.
Leveranciersrelaties	20	Nuffic moet minimaal jaarlijks de mogelijkheid krijgen om een audit te doen of uit te laten voeren op alle vereisten zoals vermeld in de overeenkomst. Bevindingen vanuit audits waaruit niet naleving van de in de overeenkomst opgenomen eisen voor informatiebeveiliging & privacy blijkt dienen onmiddellijk of binnen een met Nuffic afgestemde termijn te worden verholpen.
Leveranciersrelaties	21	Andere partijen dan onderdeel van de overeenkomst zullen geen data of toegang tot systemen met data van Nuffic ontvangen van de dienstverlener, tenzij hier expliciet en schriftelijke toestemming voor is verkregen vanuit de Information Security Officer van Nuffic.
Leveranciersrelaties	22	Indien het de dienstverlener wordt toegestaan om aan derden informatie door te geven dan dient de dienstverlener alle vereisten op gebied van informatiebeveiliging & privacy zoals opgenomen in de overeenkomst vast te leggen in contractueel overeengekomen afspraken met deze derde partij(en). De eerste dienstverlener blijft verantwoordelijk en aansprakelijk voor de juiste naleving van de uitvoering van de contractuele afspraken.
Leveranciersrelaties	23	Nuffic moet, in aanvulling op de mogelijkheid een audit uit te (laten) voeren, in staat worden gesteld om gedurende of na informatiebeveiligingsincidenten controles uit te voeren op de naleving van de in de overeenkomst genoemde vereisten.
Leveranciersrelaties	24	Het niet voldoen aan de in de overeenkomst opgenomen eisen voor informatiebeveiliging & privacy kan leiden tot beëindiging van het contract.
Leveranciersrelaties	25	Leverancier dient Nuffic proactief te informeren over wijzigingen in de organisatie die de dienstverlening gaan raken of ontdekte risico's die de dienstverlening kunnen beïnvloeden. Contractueel wordt met leveranciers overeengekomen dat ze ons op van hun belangrijke wijzigingen in hun bedrijfsvoering op de hoogte brengen.
Leveranciersrelaties	26	Ieder informatiebeveiligingsincident, data lek of vermoedelijk incident gerelateerd aan de vertrouwelijkheid, integriteit of beschikbaarheid VAN NUFFIC DATA/DIENSTVERLENING zal direct en zonder onnodige vertraging en altijd binnen 24 uur gemeld worden aan de information security officer van Nuffic via (securityofficer@nuffic.nl)

Beheer van informatiebeveiligingsincidenten	27	De opdrachtnemer neemt in alle redelijkheid maatregelen om de integriteit en beschikbaarheid van de data te garanderen. De hersteltijd bij calamiteiten is maximaal een week. De opdrachtnemer moet op enige wijze aan Nuffic aantoonbaar kunnen maken dat dit is geborgd en periodiek wordt geverifieerd en geëvalueerd.
Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	28	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. Gegevens in rust of in bewerking (incl. backups) dienen altijd binnen EU-grenzen te blijven. Gegevens in rust of in bewerking (incl. backups) dienen altijd binnen EU-grenzen te blijven.
Naleving	29	Geleverde applicaties, Clouddiensten en/of websites worden periodiek (jaarlijks) gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten. In onderling overleg wordt afgesproken binnen welke termijn de bevindingen moeten worden opgelost. Hierbij dienen bevindingen hoger dan "laag" geclassificeerd (CVSS 3.9 en hoger) binnen een maand verholpen te zijn. Bevindingen die geclassificeerd zijn als "hoog" (CVSS 4.0 - 6.9) binnen een week en als "kritiek" binnen 24 uur. Indien dit niet mogelijk is dient direct contact opgenomen te worden met de security officer van Nuffic via securityofficer@nuffic.nl