www.epnuffic.nl

P.O. Box 29777
2502 LT The Hague / The Netherlands

Baseline van informatiebeveiligingsmaatregelen

Datum	:	15-09-2015
Versie	:	1.4
Auteur	:	Team ICT

Opgesteld voor:

EP-Nuffic

Vastgesteld door:

DO

Inhoudsopgave

Inleiding

Binnen EP-Nuffic wordt uitgegaan van twee beveiligingsniveaus voor gegevens/applicaties/processen.

1. Een standaardniveau van beveiliging, geheten “baseline van maatregelen”
2. Een verhoogd niveau van beveiliging, door additionele maatregelen bovenop de standaard maatregelen.

Dit document gaat over de baseline van maatregelen. De additionele maatregelen worden beschreven in een afzonderlijk document.

De baseline van maatregelen bestaat uit procedurele en technische maatregelen die in de dagelijkse praktijk nodig zijn om een standaardniveau van informatiebeveiliging te kunnen waarborgen. Deze maatregelen vloeien voort uit het Informatiebeveiligingsbeleid. Deze basismaatregelen dienen organisatiebreed genomen te worden.

EP-Nuffic hanteert een methode om te bepalen of informatie volgens de baseline of additioneel beveiligd dient te worden. Zij classificeert informatie per proces op vereist beveiligingsniveau. Hierbij worden twee factoren gewogen:

1. het risicoprofiel van het proces;
2. het niveau voor beveiliging van persoonsgegevens .

In het Informatiebeveiligingsbeleid is deze methode uitgewerkt.

De baseline maatregelen komen met name voort uit de Wet Bescherming Persoonsgegevens (Wbp) en zijn onder te verdelen in:

1. Beveiligingseisen ten aanzien van personeel
2. Maatregelen voor de fysieke beveiliging van EP-Nuffic en haar omgeving
3. Maatregelen in het beheer van communicatie- en bedieningsprocessen
4. Toegangsbeveiligingsmaatregelen
5. Beveiligingseisen voor verwerving, ontwikkeling en onderhoud van informatiesystemen
6. Continuïteitsmanagement
7. Maatregelen voor naleving

<u>Leeswijzer</u>

Door de toevoeging van actor en scope is het eenvoudig voor de betrokken partijen af te leiden welke gedeelte van de baseline van maatregelen voor hen van toepassing is.

Per maatregel wordt aangegeven welke actoren betrekking hebben op de implementatie van een maatregel.
Een actor is een functionaris of organisatie die betrokken is bij de implementatie van een maatregel. Voor de meeste maatregelen geldt dat de proceseigenaren verantwoordelijk zijn. De proceseigenaren worden in principe daarom niet bij de actoren vermeld. De Functioneel beheerder en (ICT)projectleider hebben veelal een sturende rol en dienen derhalve kennis te nemen van alle maatregelen. Zij worden

alleen bij de maatregelen vermeld als zij een uitvoerende rol hebben. Waar medewerker staat geldt de maatregel ook voor tijdelijk personeel.
Actoren bij de baseline van maatregelen zijn medewerker, proceseigenaar, Functioneel beheerder (super user), (ICT)projectleider, Security Manager, Team ICT, HRM, JZI, Team Facilitair, externe medewerkers, externe hostingleverancier, externe softwareleverancier en clouddienst aanbieder .
De clouddienst aanbieder dient te voldoen aan de maatregelen waar externe hostingleverancier wordt vermeld.

Hiernaast wordt per maatregel ook de scope aangegeven (geldt alleen voor binnen EP-Nuffic, extern etc.).

Actualisering baseline

De baseline wordt ontwikkeld door Team ICT en goedgekeurd door de DO.

1. Definities

Active directory	centrale rechten- en beheerdatabase van het EP-Nuffic netwerk.
Autorisatiemaxtrix	matrix waarin rollen en rechten van gebruikers zijn vastgelegd.
Infrastructuur	verzameling voorzieningen die gebruikt worden voor datatransport. Hieronder vallen interne netwerken en telefoonlijnen, maar ook externe verbindingen voor o.a. internet, telefonie, VPN-verbindingen of andere communicatielijnen.
LAN	Local area network, het intern beschermde network.
Security manager	adviseert over baseline en additionele maatregelen en rapporteert over de voortgang. Verantwoordelijk voor de afhandeling van security incidenten.
Technische beheerorganisatie	organisatie die het technische beheer uitvoert (Team ICT dan wel externe hostingleverancier)
Vertrouwelijke gegevens	gevoelige gegevens/informatie, bijvoorbeeld medische gegevens, paspoortgegevens**.**

Medewerkers	in dienst van EP-Nuffic
Tijdelijk personeel	personen die worden ingehuurd
Externe medewerkers	medewerkers van externe organisaties die binnen een applicatie samenwerken met EP-Nuffic
Klanten	personen die een dienst afnemen van EP-Nuffic
Beheerders	personen die de IT infrastructuur, middelen en/of applicaties beheren

2. Beveiligingseisen ten aanzien van personeel

Medewerkers vormen een belangrijke, zo niet de belangrijkste schakel in informatiebeveiliging.

2.1 Bewustwording informatiebeveiliging

Medewerkers zijn zich bewust van het belang van informatiebeveiliging, informeren zich over beveiligingsmaatregelen en passen het informatiebeveiligingsbeleid in hun werkzaamheden toe.

2.2 Functiescheiding

Functiescheiding is verplicht voor voor medewerkers die werken aan applicaties/activiteiten die betrekking hebben op informatieverwerking. Dit houdt in dat taken betreffende de uitvoering, controle en fiattering niet door dezelfde persoon worden uitgevoerd. Functiescheidingen zijn het uitgangspunt in de procesbeschrijvingen in MAVIM.

Actoren: Proceseigenaar
Scope: EP-Nuffic, extern

2.3 Geheimhouding

Medewerkers tekenen bij aanname de arbeidsovereenkomst, waarin tevens de geheimhoudingsplicht van artikel 1.16 uit de CAO van toepassing is.

In de overeenkomst met onderstaande organisaties is voorzien dat medewerkers, die werkzaamheden voor EP-Nuffic verrichten, een geheimhoudingsplicht hebben:
-intermediair (uitzendbureau, detacheringsbureau)
-externe softwareleverancier
-externe hostingleverancier
Indien in de overeenkomst hierin niet is voorzien, dienen de medewerkers een geheimhoudingsverklaring te ondertekenen.

Externe medewerkers ondertekenen een geheimhoudingsverklaring voor beheer van systemen die een onderdeel zijn van de EP-Nuffic infrastructuur.

Actoren: Proceseigenaar
Scope: EP-Nuffic, extern

3. Maatregelen voor de fysieke beveiliging van EP-Nuffic en haar omgeving

Informatie moet niet alleen in technische- en organisatorische zin beveiligd zijn, er is ook een passende fysieke beveiliging van de informatie binnen EP-Nuffic en haar omgeving, zoals bij externe hostingleveranciers, noodzakelijk.
Zo dienen het gebouw en IT infrastructuur tegen de gevolgen van brand, waterschade, inbraak, stroomstoring etc. beschermd te worden.

3.1 Werkplek

Werkplekken binnen en buiten kantoor worden zoveel mogelijk leeg achtergelaten en apparatuur gelockt wanneer de medewerker niet bij de werkplek aanwezig is.

Actor: medewerker
Scope: EP-Nuffic, extern

3.2 Fysieke toegangscontrole

Ruimten met ICT infrastructuur zijn afgeschermd door toegangscontrole, zodat alleen bevoegd personeel toegang kan krijgen.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

3.3 Serverruimte

Er worden maatregelen getroffen om de serverruimte te beveiligen tegen calamiteiten:

- Er zijn een temperatuur- en rookmelder aanwezig;
- De airconditioning is dubbel uitgevoerd;
- Er is een blusinstallatie aanwezig;
- Medewerkers van de technische beheersorganisatie en de gebouwbeheerder hebben toegang;
- De serverruimte is voorzien van inbraakdetectie;

Actor: Team Facilitair, externe hostingleverancier
Scope: EP-Nuffic, extern

3.4 Het plaatsen en beveiligen van apparatuur

Apparatuur is zodanig geplaatst en beveiligd dat de risico's van gevaren van buitenaf en de kansen op gebruik door ongeautoriseerde personen minimaal zijn. Ook moet de (rand)apparatuur bij plaatsing niet worden beschadigd. Het plaatsen van computerapparatuur dient alleen te worden uitgevoerd volgens de aanwijzingen van de fabrikant, door bevoegd onderhoudspersoneel onder toezicht van medewerkers van de technische beheersorganisatie.

Actor: medewerker, externe medewerker, Team ICT
Scope: EP-Nuffic

3.5 Onderhouden van apparatuur

Apparatuur moet volgens de aanwijzingen van de fabrikant onderhouden en gerepareerd worden, door bevoegd onderhoudspersoneel onder toezicht van medewerkers van de technische beheersorganisatie.

Om de werking van bedrijfskritische apparatuur te waarborgen wordt er gebruik gemaakt van onderhoudscontracten en reserve-apparatuur.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

3.6 Gegevens verwijderen

Voordat apparatuur en media worden afgevoerd dienen de opgeslagen gegevens te worden verwijderd. Dit dient te worden uitgevoerd of goedgekeurd door Team ICT of de externe hostingleverancier. Indien privé apparatuur die voor EP-Nuffic wordt gebruikt, wordt verkocht of indien de medewerker uit dienst treed worden EP-Nuffic gegevens door de medewerker verwijderd.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

3.7 Uitlenen en in bruikleen geven van apparatuur en informatiedragers

Bij het uitlenen en in bruikleen geven van apparatuur en informatiedragers, is de medewerker verantwoordelijk om zorgvuldig met de apparatuur en informatiedragers om te gaan en deze niet onbeheerd achter te laten, dan wel uit te lenen of te laten gebruiken door derden. Denk hierbij bijvoorbeeld aan objecten zoals laptops, notebooks, smartphones en externe harddisks.

Er is een uitleenbeheer van apparatuur.
De medewerker tekent gebruiksvoorwaarden t.b.v. de bruikleen van apparatuur.

Actor: medewerker
Scope: EP-Nuffic, extern

3.8 Stroomvoorziening

Bedrijfskritische apparatuur is beveiligd tegen stroomstoringen. Bedrijfskritische apparatuur is aangesloten op een noodstroomvoorziening.

Actor:Team Facilitair, externe hostingleverancier
Scope: EP-Nuffic, extern

4. Maatregelen in het beheer van communicatie- en bedieningsprocessen

Via IT-voorzieningen zoals interne- en externe netwerken en systemen en mobiele apparatuur wordt veel informatie verspreid. Deze IT- voorzieningen dienen veilig bediend en beheerd te worden.

4.1 Opslag data

Data wordt zo min mogelijk lokaal op mobiele apparatuur of werkstations opgeslagen en alleen op het netwerk, one drive, Sharepoint of een andere door EP-Nuffic aangeboden cloudvoorziening in overleg met ICT.
Voor opslaan in de cloud geldt, dat de cloudvoorziening voldoet aan het Informatiebeveiligingsbeleid.

Actor: medewerker, Team ICT
Scope: EP-Nuffic, extern

4.2 Restrictie in opslagcapaciteit werkstations

Om te voorkomen dat gebruikers teveel data opslaan op het netwerk, wordt gewerkt met opslaglimieten. In het EP-Nuffic netwerk is de maximum opslag standaard 15GB per gebruiker.

Actor: Team ICT
Scope: EP-Nuffic

4.3 Opslag audio en video bestanden

Gebruikers kunnen enkel op de shared mappen op het netwerk audio en video bestanden opslaan of in een door EP-Nuffic aangeboden cloudoplossing

Actor: medewerker, Team ICT
Scope: EP-Nuffic, extern

4.4 Installatie van software

Gebruikers kunnen op in bruikleen gegeven mobiele apparatuur, apps installeren indien deze uit een officiële appstore komen, uit betrouwbare- en bekende bron komen en geen veiligheidsrisico's opleveren.

Actor: medewerker
Scope: EP-Nuffic, extern

4.5 Clouddiensten

Clouddiensten zijn software-, platforms- of infrastructuurdiensten die op aanvraag via het internet beschikbaar gesteld worden. Deze diensten zijn makkelijk schaalbaar afhankelijk van de behoefte van de klant. Clouddiensten kenmerken zich door meerdere grote datacenters zodat de continuïteit van diensten gewaarborgd is en de diensten aan meerdere klanten kunnen worden aangeboden. Clouddiensten vereisen een aantal specifieke beveiligingsmaatregelen bovenop de in de Baseline omschreven maatregelen met een externe scope.

- Voordat een clouddienst wordt afgenomen wordt een risico-analyse gedaan, die gebaseerd is op de “Whitepaper NCSC Cloudcomputing security Bijlage E Handige vragen en aandachtspunten”. – januari 2012. Op basis van deze analyse zullen de vereiste beveiligingsmaatregelen worden genomen.

- Opslaan van EP-Nuffic gegevens in een clouddienst is alleen toegestaan als deze dienst voldoet aan het Informatie beveiligingsbeleid van EP-Nuffic.
  Gevoelige gegevens mogen niet in de cloud worden opgeslagen.
  Gevoelige gegevens zijn bijvoorbeeld paspoort gegevens en medische gegevens. Of gegevens gevoelig zijn wordt d.m.v. een classificatiemethode bepaald (zie hiervoor het Informatiebeveiligingsbeleid, paragraaf 2.2).

- Vanwege de rechtsbescherming van gegevens is is het is van belang om vast te leggen in welke landen/regio’s de gegevens (incl. backups) worden opgeslagen of naar welke landen/regio’s ze worden geëxporteerd Dit dient de Europese Unie te zijn en bij voorkeur Nederland, vanwege de Nederlandse rechtsbescherming. Bij hosting in andere landen dan Nederland worden JZI en Team ICT gevraagd te adviseren over de rechtsbescherming van gegevens.

- Met de cloudleverancier dienen afspraken te worden gemaakt dat de vernietiging van gegevens conform
  Wbp en Archiefwet en -beleid plaatsvinden.

- De clouddienst aanbieder moet aangeven hoe de toegang tot de data is geregeld, m.b.t. autorisaties voor eigen medewerkers en hoe EP-Nuffic bij de data komt.

- De clouddienst aanbieder en haar eventuele partners worden jaarlijks extern geaudit en beschikken over een ISO 27002 en ISAE 3402 of SSAE 16 (SOC1) Type II certificering. EP-Nuffic kan deze auditresultaten opvragen.

Actor: Functioneel beheerder en (ICT)projectleider zijn verantwoordelijk voor applicaties van afdelingen in de cloud en voor het maken van genoemde risicoanalyse op grond van de Whitepaper NCSC Cloudcomputing security in overleg met Team ICT
Actor: Team ICT is verantwoordelijk voor EP-Nuffic brede applicaties en voor beoordelen risico analyse op grond van genoemde Whitepaper NCSC Cloudcomputing security
Actor: clouddienst aanbieder
Scope: EP-Nuffic, extern

LET OP: tevens dient de Clouddienstaanbieder aan de maatregelen te voldoen waar externe hostingleverancier bij wordt vermeld.

4.6 Toegankelijkheid informatie

De informatie op opslagmedia en in applicaties dient gedurende de gehele bewaarperiode toegankelijk te blijven (leesbaarheid van zowel media als gegevensformaat). Dit om te voorkomen dat de informatie verloren gaat als gevolg van toekomstige technologische veranderingen, zoals bij veranderingen in gegevensformaat, nieuwe releases etc.

Actor: Functioneel beheerder, Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

4.7 Back-ups

Om te voorkomen dat er gegevens verloren gaan na een calamiteit worden er regelmatig back-ups gemaakt. Er zijn procedures beschreven voor back-ups en recovery schema's.

Back-ups zijn versleuteld. Aangegeven wordt hoe back-ups zijn versleuteld. De bewaarlocatie van back-ups bevindt zich buiten de locatie waar de verwerking van gegevens plaatsvindt.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

Indien data op mobiele apparatuur wordt opgeslagen wordt altijd zorggedragen voor een periodieke back-up.

Actor: medewerker
Scope: EP-Nuffic, extern

Waar data op de werkstations moet worden opgeslagen is een voorziening getroffen voor het maken van back-ups in overleg met ICT. Bij hoge uitzondering komt een backup van een lokale applicatie wel op een werkstation.

Actor: medewerker, Functioneel beheerder (back-up op lokale werkstations)
Scope: EP-Nuffic

4.8 Vernietiging van (persoons)gegevens

Persoonsgevens worden niet langer bewaaard dan voor het doel waarvoor ze benodigd zijn. Er worden voldoende maatregelen genomen om te voldoen aan de wettelijke vernietigingsplicht volgens de Archiefwet en Wbp. De opslagduur van digitale paspoortkopieën wordt geminimaliseerd en zodra identificatie t.b.v. een beurs of diplomawaardering en bijvoorbeeld verblijfvergunning t.b.v. kandidaten heeft plaatsgevonden, worden digitale paspoortkopieën verwijderd, of indien dat onmogelijk is wordt het BSN en/of foto afgeschermd.

Actor: proceseigenaar, externe hostingleverancier
Scope: EP-Nuffic, extern

4.9 Synchronisatie van systeemklokken

Systeemklokken worden tenminste dagelijks gesynchroniseerd.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

4.10 Gebruik ICT-voorzieningen en informatie

Medewerkers dienen zorgvuldig om te gaan met de door EP-Nuffic aan hen beschikbaar gestelde kantoor en ICT voorzieningen en apparatuur en ook met de EP-Nuffic informatie die ze op EP-Nuffic

apparatuur en privé apparatuur gebruiken. Dit houdt tevens in dat laatste updates en versies van Operating systems en beveiligingssoftware worden geïnstalleerd.

Actor: medewerker
Scope: EP-Nuffic, extern

Voor het gebruik en beheer van de applicaties en ICT-voorzieningen dienen adequate instructies/handleidingen beschikbaar te zijn.

Actor: Functioneel beheerder, Team ICT, externe softwareleverancier, externe hostingleverancier
Scope: EP-Nuffic, extern

4.11 Bescherming intellectueel eigendom eigen applicaties

Indien EP-Nuffic maatwerk laat ontwikkelen, draagt zij er zorg voor dat de broncode op afdoende wijze technisch wordt beschermd tegen inbreuk van derden. De toegang tot de broncode behoort te worden afgeschermd en de actualisatie ervan kan alleen worden uitgevoerd door daartoe geautoriseerde personen. De productieomgeving werkt met een afgeleide code die niet terug te herleiden is naar de originele broncode.

Actor: (ICT)projectleider, externe softwareleverancier
Scope: EP-Nuffic, extern

4.12 Viruscontrole

Alle werkstations, door EP-Nuffic in bruikleen gegeven apparatuur en privé apparatuur met EP-Nuffic informatie, zijn voorzien van bijgewerkte antivirusprogrammatuur. Privé apparatuur is ingesteld volgens de beveiligingsinstellingen die door de fabrikant zijn aanbevolen. Voor werkstations vindt periodiek rapportage aan de Security Manager plaats. Deze programmatuur wordt tenminste één keer per week voorzien van updates. Systeembestanden kunnen uitgesloten zijn van controle om dataverlies door een storing van de antivirusprogrammatuur te voorkomen.

Netwerkverkeer kan ook gecontroleerd worden op virussen.

Actor: medewerker, Team ICT
Scope: EP-Nuffic, extern

4.13 Spam-en cookiebeleid

EP-Nuffic voldoet aan de vereisten uit de Telecommunicatiewet dat er geen ongevraagde e-mail berichten gestuurd mogen worden aan particulieren of niet-natuurlijke rechtspersonen en niet ongevraagd cookies op hun apparatuur mogen worden geplaatst. EP-Nuffic plaatst standaard een “opt out” mogelijkheid in een mailing. De “opt out” mogelijkheid is een uitzondering op de hoofdregel dat expliciet toestemming gevraagd moet worden. Uitgangspunt hierbij is dat EP-Nuffic haar contactgegevens altijd verkrijgt “in het kader van de verkoop van een dienst of product”, namelijk in het kader van de dienst “internationalisering van hoger onderwijs”.
EP-Nuffic vraagt gebruikers toestemming voor het plaatsen van niet functionele cookies (o.a. cookies van derden zoals social media). Daarnaast informeert zij gebruikers over het gebruik van cookies.

Actor: medewerker
Scope: EP-Nuffic

4.14 Beveiliging Smartphones / laptops / tablets / notebooks / privé apparatuur

- Bij diefstal van een smartphone, laptop, tablet, notebook of privé apparatuur met EP-Nuffic informatie en programmatuur, dient dit onmiddellijk aan de Security manager gemeld te worden. Apparatuur die op afstand wordt beheerd zal dan een wisopdracht worden gestuurd.

Actor: medewerker, Team ICT
Scope: EP-Nuffic, extern

- Mobiele apparatuur dient versleuteld te zijn. Indien voor smartphones gebruik wordt gemaakt van activesync (synchronisatie mail en agenda's) wordt de smartphone geheel versleuteld en van een vier cijferige pincode voorzien. Na 9 inlogpogingen worden alle gegevens gewist en wordt de telefoon in fabriekstoestand teruggezet. Er zijn geen andere protocollen dan activesync toegestaan voor smartphones

Actor: medewerker, Team ICT
Scope: EP-Nuffic, extern

4.15 Gebruik van e-mail

Gebruikers dienen op de hoogte te zijn van de kwetsbaarheden van e-mail zonder versleuteling.

- Het juridische EP-Nuffic beleid met betrekking tot e-mail wordt standaard aan ieder uitgaand bericht toegevoegd (disclaimer).
- E-mail wordt gescand op virussen.
- Het via het EP-Nuffic e-mail systeem versturen van programmatuur, bestanden die niet kunnen worden gecontroleerd op virussen en multimedia bestanden worden automatisch geblokkeerd.
- Het is binnen EP-Nuffic niet toegestaan om via Outlook of andere desktopprogrammatuur een bulkmailing te doen naar honderd of meer geadresseerden.
- Volgens de baseline geclassificeerde gegevens mogen verzonden worden via de mail mits deze versleuteld is via S/MIME of Office 365.

Actor: medewerker, Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

4.16 Beveiliging netwerkverkeer

Voor het versturen van EP-Nuffic informatie worden beveiligde verbindingen gebruikt.

De beveiliging van webverkeer dient te worden getoetst door de site te testen via de website: ssllabs.com. Er dient ten minste een B score te worden behaald.

Bovendien dienen onbeveiligde verbindingen te worden geblokkeerd of omgeleid naar een beveiligde verbinding om onbeveiligd transport uit te sluiten.

Actor: externe hostingleverancier, Team ICT
Scope: EP-Nuffic, extern

4.17 Beperkingen toegang tot niet geautoriseerde programmatuur (alleen EP-Nuffic LAN)

Om de verspreiding van virussen en andere kwaadaardige programmatuur tegen te gaan zijn er een aantal maatregelen getroffen:

- Het downloaden van programmatuur is geblokkeerd in de firewall;
- Er is een zogenaamde group policy voor alle werkstations die het starten van programmatuur van USB sticks en overige mobiele media zoveel mogelijk blokkeert;
- Het installeren van zogenaamde ActiveX Controls is voor de gebruikers niet mogelijk zonder dat dit is vrij gegeven door de netwerkbeheerder. Voor de vrijgave van een ActiveX control dient de wijzigingenbeheerprocedure te worden doorlopen. Alleen trusted of signed ActiveX controls van gerenommeerde externe softwareleveranciers komen in aanmerking voor installatie na beoordeling door de technische beheerorganisatie op beveiliging en operationele aspecten;
- De netwerkbeheerder kan ongeautoriseerde programmatuur blokkeren door het digitale certificaat van een externe softwareleverancier in de Active Directory op te nemen als niet toegestaan.

Actor: Team ICT
Scope: EP-Nuffic

4.18 Afscherming EP-Nufficnetwerk

Het netwerk is afgeschermd van andere netwerken door een firewall die volgens het nee tenzij principe is geconfigureerd.

Er zijn diverse zones ingericht om het binnendringen van kwaadwillenden te bemoeilijken.

- Voor diagnose van netwerkproblemen kan door de netwerkbeheerder gebruik gemaakt worden van de logboeken van de firewall.
- Deze logboeken houden de acties aangaande inkomend en uitgaand netverkeer bij, niet de data zelf.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

Additioneel gelden de volgende eisen bij het EP-Nuffic netwerk:

- Het initiëren van verbindingen door derden, rechtstreeks naar systemen binnen het LAN, is niet toegestaan.
- HTTPS verbindingen naar EP-Nuffic systemen waarbij AD authenticatie door de firewall wordt gedaan zijn eventueel wel toegestaan. Het dient hier dan wel om individuele AD gebruikersaccounts te gaan. De verbinding moet bovendien gebruik maken van de https publishing faciliteit van de firewall.
- Alle systemen die rechtstreeks benaderbaar moeten zijn door systemen van buiten het EP-Nuffic netwerk (LAN) zijn in een afgeschermde zone geplaatst, de DeMilitarized Zone. Systemen die in de DMZ staan mogen niet gebruikt worden om gegevens in op te slaan.
- Het is niet toegestaan om externe systemen te koppelen aan het LAN (VPN) tenzij toegestaan door ICT.

- Toegang op afstand voor medewerkers is alleen toegestaan op basis van AD authenticatie door de firewall. Toegang op afstand voor externen kan gefaciliteerd worden in overleg met ICT.

Actor: Team ICT
Scope: EP-Nuffic

4.19 Beheer computersystemen

Systeembeheertaken mogen alleen worden uitgevoerd door de technische beheersorganisatie, met voldoende gekwalificeerde systeembeheerders.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

4.20 Beleid beveiligingsupdates en aanbevelingen

Het beschikbaar zijn van security updates en security aanbevelingen van de fabrikant moeten beiden actief worden gemonitord door de technische beheerorganisatie en op redelijke termijn worden geïmplementeerd.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

Er is een update management tool voor alle Microsoft programmatuur.

Actor: Team ICT
Scope: EP-Nuffic

4.21 Extern gehoste systemen

Bij extern gehoste systemen is de externe technische beheersorganisatie belast met de uitvoering van de beveiliging en dient op aanvraag van de Security manager hierover te rapporteren aan de Proceseigenaar en de Security manager.

Actor: externe hostingleverancier
Scope: extern

4.22 Security incidenten

Security incidenten en inbreuk incidenten (waaronder inbreuken op de beveiliging van (persoons)gegevens worden zo spoedig mogelijk en tenminste op de dag van ontdekking bij de Proceseigenaar en de Security manager gemeld. Tevens wordt aangifte bij de politie gedaan in geval van diefstal of het hacken van applicaties/sites. Een kopie van het proces verbaal hiervan wordt aan team Juridische Zaken Inkoop gegeven. De Security manager registreert de incidenten. De security incidenten worden afgehandeld en dienen als input voor de incident-rapportages.

Zie ook: hoofdstuk 6 Informatiebeveiligingsbeleid.

Actor: medewerker, externe hostingleverancier, Security manager
Scope: EP-Nuffic, extern

5. Toegangsbeveiligingsmaatregelen

5.1 Procedure in- en uitdiensttreding & functiewijzigingen

Gebruikersaccounts worden aangemaakt conform de procedure voor In- en uitdiensttreding en functiewijzigingen (voor applicaties en shared) en procedure Tussentijdse aanvragen voor shared directories en applicaties.

Gebruikersaccounts voor NESO medewerkers worden op voorstel van een NESO directeur en na accordering door Hoofd Positionering aangemaakt en verwijderd.

Voor externe medewerkers en extern ingehuurd personeel wordt voor het definiëren en toekennen van bevoegdheden een overeenkomstige procedure als voor het eigen personeel toegepast.

Actor: HRM, proceseigenaar, Team ICT. Functioneel beheerder
Scope: EP-Nuffic, extern

5.2 Autorisatiematrix

Per informatiesysteem wordt door de Functioneel beheerder een matrix gemaakt en beheerd. In de matrix worden de functies en rollen met elkaar in verband gebracht. Deze moeten gelijklopen met de functies en rollen die zijn vastgelegd in de AO van de afdeling of in de procesbeschrijvingen.

De matrix is zo de leidraad en het controlemiddel om de gevraagde autorisatie wel of niet toe te kennen. De matrix wordt goedgekeurd door de Proceseigenaar. De matrix mag alleen worden aangepast na goedkeuring van de Proceseigenaar.

De rol van de beheerder van een applicatie (netwerkbeheerder, databasebeheerder, externe medewerker en Functioneel beheerders) moet duidelijk worden omschreven en gedocumenteerd. De netwerk administrator dient goed te zijn geïnstrueerd. Er dient gewerkt te worden volgens gedocumenteerde rollen.

Actor: Functioneel beheerder, proceseigenaar
Scope: EP-Nuffic

5.3 Beveiligde verbinding inlogprocedures

Voor inlogprocedures (gebruikersnaam en wachtwoorden) is het gebruik van beveiligde verbindingen verplicht. Gebruikersnaam en wachtwoorden mogen enkel verzonden worden door ze tijdens de gehele transportketen te beveiligen met een actueel, sterk versleutelingsalgoritme.

Actor: Functioneel beheerder, Team ICT
Scope: EP-Nuffic, extern

5.4 Verbindingen met derden

Alleen na een geautoriseerde aanvraag van de proceseigenaar krijgen derden toegang tot informatievoorzieningen, via een remote desktop tool.

Om deze risico's te beperken wordt gebruik gemaakt van beveiligde verbindingen

Actor: Functioneel beheerder, Team ICT
Scope: EP-Nuffic

5.5 Beveiliging van systeemdocumentatie

Systeemdocumentatie wordt beschermd tegen ongeautoriseerde toegang want deze documentatie kan gevoelige gegevens bevatten. Systeemdocumentatie wordt opgenomen in een afgeschermd gedeelte van het netwerk.

Actor: Functioneel beheerder, externe hostingleverancier, team ICT
Scope: EP-Nuffic, extern

5.6 Accounts voor externe medewerkers

Externe medewerkers dienen accounts te gebruiken die op naam zijn gesteld.

Actor: externe medewerkers
Scope: EP-Nuffic, extern

5.7 Opheffen accounts voor netwerk en applicaties

Accounts voor het netwerk en applicaties worden, na de laatste werkdag van medewerkers, tijdelijk personeel of externe medewerkers, geblokkeerd. Na maximaal één maand wordt het account verwijderd. De Procedure voor In- en uitdiensttreding en functiewijzigingen is van toepassing. Periodiek wordt op ongebruikte useraccounts gecontroleerd en worden deze verwijderd.

Actor: Functioneel beheerder (super user), Team ICT, HRM, proceseigenaar
Scope: EP-Nuffic, extern

5.8 Gebruikersrechten medewerkers

Alle medewerkers werken op desktops, laptops en tablets met standaard gebruikersrechten.

Actor: Team ICT
Scope: EP-Nuffic

5.9 Wachtwoorden voor applicaties en netwerktoegang

5.9.1 Algemeen

- Een wachtwoord wordt beschouwd als vertrouwelijke informatie en mag niet gedeeld worden met anderen.
- Indien een wachtwoord niet in de AD is opgenomen dient deze als volgt beveiligd te zijn:
  - Er wordt gebruik gemaakt van hashing met het bcrypt algoritme;
  - Er wordt gebruik gemaakt van een per user salt van 64 bits of meer.
- Toegangsautorisatie tot applicaties gehost bij EP-Nuffic verloopt via de Active Directory
- Toegansautorisatie voor systemen die extern gehost zijn voor medewerkers verloopt via Azure AD

- Eerder gebruikte wachtwoorden zijn niet toegestaan (met een historie van minimaal tien);
- Een nieuwe medewerker is verplicht het eenmalige wachtwoord direct te wijzigen.

Aanvullend gelden de volgende wachtwoord policies:

Klanten:	Wachtwoorden zijn minimaal 6 tekens;
Externe medewerkers:	Wachtwoorden zijn minimaal 8 tekens;
Medewerkers:	Wachtwoorden zijn minimaal 8 tekens en levensduur van het wachtwoord is 6 maanden

Actor: Functioneel beheerder (super user), Team ICT, externe hostingleverancier, externe softwareleverancier
Scope: EP-Nuffic, extern

5.9.2 Beheer van Activedirectory wachtwoorden

- Activedirectorywachtwoorden worden beheerd door de netwerkbeheerder of beheerders van specifieke Organisatie units aan wie dit gedelegeerd is door de netwerkbeheerder;
- Een wachtwoord van een EP-Nuffic medewerker kan op verzoek van een derde alleen gereset worden met toestemming van de leidinggevende;
- Na vijf mislukte aanmeldpogingen wordt een medewerkersaccount automatisch 30 minuten vergrendeld;

Actor: Team ICT, functioneel beheerder
Scope: EP-Nuffic

5.9.3 Beheerders van applicaties

- Wachtwoorden in applicaties worden beheerd door de Functioneel beheerders.

Actor: Functioneel beheerder (super user)
Scope: EP-Nuffic

5.9.4 Klanten

- Gebruikers, zonder Active Directory account, krijgen bij het aanmaken van een account een eenmalig wachtwoord toegezonden dat bij het aanmelden dient te worden gewijzigd;
- Indien zo'n gebruiker zijn geregistreerde wachtwoord vergeten is kan hij zelf online binnen de applicatie een nieuw eenmalig wachtwoord aanvragen, dat wordt gemaild naar het oorspronkelijke e-mail adres. Indien bovengenoemde automatische online procedure binnen de applicatie niet werkt kan de gebruiker contact opnemen met de Functioneel beheerder/Super user om het wachtwoord en/of e-mail adres te laten wijzigen. De Functioneel beheerder/Super user dient volgens zich te vergewissen dat het verzoek authentiek is en kan worden uitgevoerd.
- Een aanmeldfunctionaliteit van sociale media sites mag gekoppeld worden aan een EP-Nuffic site/applicatie mits dit goedgekeurd is door de Security manager.

Actor: Functioneel beheerder (super user), Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

5.10 Wachtwoorden mobiele apparatuur

Voor een smartphone is een pincode van minimaal vier tekens verplicht .
Na 15 minuten inactiviteit wordt opnieuw ingelogd met een pincode.
Bij diefstal of verlies van de apparatuur wordt het wachtwoord direct via de self service gewijzigd.

Actor: medewerrker
Scope: EP-Nuffic, extern

5.11 Time-out voor werkstations

Werkstations worden na 30 minuten automatisch vergrendeld om toegang door onbevoegden te voorkomen.

Actor: Team ICT
Scope: EP-Nuffic

5.12 Locken van werkstations en apparatuur

Werkstations en apparatuur worden gelockt wanneer de medewerker niet in de buurt van het werkstation en apparatuur is.

Actor: medewerker
Scope: EP-Nuffic, extern

5.13 Logbestanden van netwerk

Aanmeldpogingen worden gelogd. Deze worden slechts gebruikt bij security incidenten en (geanonimiseerde) managementrapportages
Handelingen van externen voor beheer van systemen die een onderdeel zijn van de EP-Nuffic infrastructuur dienen gelogd te worden over een periode van drie maanden. Deze logfiles dienen beschermd te zijn tegen wijzigingen door deze externen.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

6. Beveiligingseisen voor verwerving, ontwikkeling en onderhoud van systemen

6.1 Selectietrajecten, ontwikkeling & onderhoud

Bij selectietrajecten voor informatiesystemen en hosts en bij ontwikkeling en onderhoud worden het Informatiebeveiligingsbeleid en de relevante informatiebeveiligingsmaatregelen altijd meegenomen.

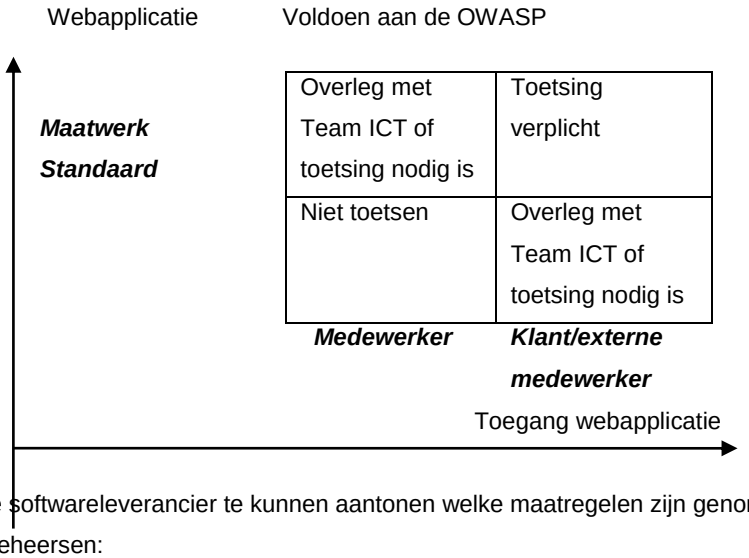
Ook wordt door Team ICT bij het eisenpakket getoetst of er sprake is van persoonsgegevens- of vertrouwelijke gegevens. De classificatiemethode, zoals beschreven in het informatiebeveilgingsbeleid, zal vervolgens worden toegepast. Indien voor de betreffende gegevens een meldplicht in het kader van de Wbp geldt, dan zal JZ hiervoor worden ingeschakeld.

Actor: (ICT)projectleider, externe softwareleverancier, externe hostingleverancier
Security manager toetst technische eisen
Team ICT toetst of er sprake is van persoonsgegevens- of vertrouwelijke gegevens
JZ toetst meldplicht persoonsgegevens
Scope: EP-Nuffic, extern

6.2 Best practices product & platform

De externe softwareleverancier dient aan te kunnen tonen dat hij zoveel mogelijk voldoet aan de best practices van het gebruikte product en platform. Dit aantonen kan voor het Microsoft platform gedeeltelijk met een zogenaamde best practices analyzer en in detail door een auditor.

Specifiek voor webapplicaties gelden een aantal beveiligingsricio's. Webapplicaties zijn applicaties die gebruikt worden binnen een webbrowser.
De beveiligingsrisico's voor webapplicaties hangen mede af van of een webapplicatie een standaard applicatie of maatwerk is en of het toegankelijk is voor medewerkers en/of klanten/externe medewerkers. Daarmee varieert ook de mate waarin webapplicaties beveiligd dienen te zijn tegen de kritische web applicatie beveiligingsrisico's (OWASP Top 10) .



Bij toetsing dient de externe softwareleverancier te kunnen aantonen welke maatregelen zijn genomen om de OWASP Top 10 te beheersen:

Deze maatregelen dienen per OWASP Top tien punt aangegeven en toegelicht te worden, en

gebaseerd te zijn op “how do I prevent …..” van het document “OWASP Top 10 -2013: the Ten Most Critical Web Applications Security Risks” / The OWASP foundation, 2013.
Voorbeeld: Voor A-3 – Cross-Site Scripting (XSS) zijn de preventieve maatregelen nummer één en twee geïmplementeerd.

Actor: (ICT)projectleider, Functioneel beheerder, Team ICT, externe softwareleverancier, externe hostingleverancier
Scope: EP-Nuffic, extern

6.3 Overzicht van bedrijfsmiddelen

Alle belangrijke informatiebedrijfsmiddelen en IT bedrijfsmiddelen zijn gedocumenteerd. Het gaat hierbij tenminste om: datamodellen, software, datacommunicatieprotocollen en ook om de niet-geautomatiseerde informatievoorziening. Dit draagt er toe bij dat alle bedrijfsmiddelen op de juiste manier beveiligd blijven. De proceseigenaren zijn hiervoor verantwoordelijk. Zie ook in vorige hoofdstuk, over de afscherming van deze documentatie.

Actor: Functioneel beheerder, Team ICT, externe softwareleverancier
Scope: EP-Nuffic (betreft maatwerk), extern (betreft maatwerk en standaardapplicaties)

6.4 Toetsing beveiliging

Het contract met de externe softwareleverancier voor de ontwikkeling van applicaties en de toegang tot informatievoorzieningen van EP-Nuffic bevat de beveiligingseisen. Met een externe softwareleverancier wordt een service level agreement (SLA) overeengekomen waarin het beheer van applicaties is geregeld, alsmede waarin de relevante beveiligingseisen zijn opgenomen, zoals het maken van back-ups en incidentbeheer.
Contracten en algemene voorwaarden worden getoetst op beveiligingseisen. . Als deze afwijken van de Informatiebeveiligingsmaatregelen wordt onderhandeld over contractaanpassing.

De projectleider waarborgt dat de externe softwareleverancier bovenstaande eisen hanteert bij de ontwikkeling/aanbod van een informatiesysteem en stemt dit af met de Security manager.

Bij de acceptatietest wordt getoetst of deze beveiligingseisen goed zijn geïmplementeerd.

Actor:(ICT)projectleider, Functioneel beheerder, externe softwareleverancier, externe hostingleverancier
Actor: Team ICT toetst contracten op beveiligingseisen
Scope: EP-Nuffic, extern

6.5 Veiligstellen data

Het contract met de externe software leverancier bevat afspraken m.b.t. de wijze waarop data retour komt in geval dat het contract beëindigd wordt of de externe software leverancier surseance van betaling aanvraagt dan wel verkrijgt of in staat van faillissement is verklaard.

Actor:(ICT)projectleider, Functioneel beheerder, externe softwareleverancier
Scope: EP-Nuffic, extern

6.6 Validatie van invoergegevens

Bij de ontwikkeling van toepassingen voor EP-Nuffic worden maatregelen genomen die de in te voeren gegevens controleren op juistheid, syntax en volledigheid.

Actor:(ICT)projectleider, Functioneel beheerder, externe softwareleverancier
Scope: EP-Nuffic, extern

6.7 Functiescheiding

Functiescheiding in AO dient zo veel mogelijk ook in systeem worden toegepast, met betrekking tot rollen en autorisatie rechten. Hiermee wordt rekening gehouden bij ontwerp en implementatie van systemen.

Actor:(ICT)projectleider, Functioneel beheerder, externe softwareleverancier, proceseigenaar
Scope: EP-Nuffic, extern

6.8 Beveiliging van testgegevens

Testgegevens moeten worden beveiligd en beheerd. Het gebruik van een identieke kopie van productie databases met gevoelige gegevens (waaronder persoonsgegevens) moet worden vermeden.

Voor het testen van informatiesystemen met persoonsgegevens en voor trainingen voor informatiesystemen worden zoveel mogelijk niet tot personen herleidbare gegevens van personen gebruikt.

Actor:(ICT)projectleider, Functioneel beheerder, P&C /ICT, externe softwareleverancier, externe hostingleverancier
Scope: EP-Nuffic, extern

6.9 Productie, test en ontwikkelomgeving

Indien programmatuur, wordt ontwikkeld of getest dient dit te gebeuren op een van de productieomgeving gescheiden (acceptatie)test- en ontwikkelomgeving (OTAP). De ontwikkel- en testomgeving zijn bij de leverancier.

Bij het overzetten van (acceptatie)test naar productieomgeving wordt gebruik gemaakt van de wijzigingenbeheerprocedure.

Actor:(ICT)projectleider, Functioneel beheerder, Team ICT, externe softwareleverancier zijn er verantwoordelijk voor dat in een test- en ontwikkelomgeving wordt getest.
Actor:Wijzigingsbeheerder beoordeelt en accordeert de wijziging, als het om binnen EP-Nuffic gehoste applicaties gaat.
Actor: Team ICT, externe hostingleverancier en externe softwareleverancier faciliteren de test- en ontwikkelomgeving en het overzetten naar de productieomgeving
Scope: EP-Nuffic, extern

6.10 Koppeling van systemen

Gekoppelde applicaties moeten allen voldoen aan de strengste eisen gesteld aan één of meerdere van de gekoppelde applicaties.

Actor:(ICT)projectleider, Functioneel beheerder, externe softwareleverancier
Scope: EP-Nuffic, extern

6.11 Koppeling van systemen

Voor de installatie van Windows en SQL server wordt de baseline gevolgd zoals beschreven in:

x:\shared\BV\P&C\ICT\Beheer\Technisch Beheer Algemeen\Baselines\

Actor: Team ICT
Scope: EP-Nuffic

7. Continuïteitsmanagement

In het continuïteitsplan worden het herstel van de infrastructuur en betrokken applicaties beschreven. Daarnaast worden een aantal preventieve maatregelen beschreven alsmede de communicatie bij een calamiteit. De herstelinspanningen en -snelheid worden gerelateerd aan de in de inleiding omschreven classificatie van gegevens, op basis waarvan de infrastructuur en applicaties als kritisch of minder kritisch worden beschouwd.

Actor: Team ICT, externe hostingleverancier
Scope: EP-Nuffic, extern

8. Maatregelen voor naleving

EP-Nuffic wil ervoor zorgen **dat wetgeving, contractuele verplichtingen en beveiligingseisen** worden nageleefd en voorkomen dat EP-Nuffic in problemen komt door niet naleving. Een goede communicatie over de verplichtingen en beveiligingseisen is essentieel.

8.1 Toezicht beveiligingseisen

Via geautomatiseerde monitoring (van het netwerk) audits, projectevaluaties en rapportages wordt toezicht gehouden op de naleving van de eisen voortvloeiend uit het Informatiebeveiligingsbeleid, baseline, additionele maatregelen en verwante procedures.

Actor: Security manager, Externe hostingleverancier
Scope: EP-Nuffic, extern

8.2 Toezicht verwerking persoonsgegevens

De naleving van de Wet Bescherming Persoonsgegevens wordt geborgd door procedures voor de verwerking van persoonsgegevens. Proceseigenaren zijn verantwoordelijk voor het toezicht op de verwerking van persoonsgegevens binnen hun afdeling en, indien de verwerking is uitbesteed aan een externe organisatie, voor het toezicht op deze externe organisatie. De externe organisatie dient te voldoen aan eisen gesteld door de Wet Bescherming Persoonsgegevens.

Actor: Proceseigenaar is verantwoordelijk voor het toezicht op de verwerking van persoonsgegevens.
Actor: P&C/JZ stelt procedures voor de verwerking van persoonsgegevens.
Scope: EP-Nuffic, extern

8.3 Intellectueel eigendom

Programmatuur wordt alleen aangeschaft via bekende en erkende externe softwareleverancieren om te waarborgen dat geen auteursrechten worden geschonden.

Actor: (ICT)projectleider en Functioneel beheerder
Scope : EP-Nuffic, extern

Licenties worden zorgvuldig beheerd. Er wordt gewaarborgd dat aan de licentievoorwaarden voldaan blijft worden. Bewijsmateriaal van het aantal en soort licenties van EP-Nuffic wordt bewaard en onderhouden.

Actor: Functioneel beheerder
Scope : EP-Nuffic, extern

8.4 Controle wachtwoorden EP-Nuffic medewerkers

De Securitymanager zal jaarlijks aan de senior IT medewerker rapporteren over het naleven van de password eisen.

Actor: Securitymanager
Scope: EP-Nuffic

8.5 Controle op het verwijderen van ongebruikte user en group objecten uit de AD

De securitymanager zal jaarlijks met de senior IT medewerker een controle uitvoeren of ongebruikte AD user en groups zijn verwijderd.

Actor: Securitymanager
Scope: EP-Nuffic