www.epnuffic.nl

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

Additionele beveiligingsmaatregelen

Datum	**:**	15-09-2015	**Opgesteld voor:**	
Versie	**:**	1.4	EP-Nuffic	
Auteur	**:**	Team ICT	**Vastgesteld door:**	
			DO	

Inhoudsopgave

Inleiding additionele beveiligingsmaatregelen

Additionele beveiligingsmaatregelen worden genomen bovenop de baseline van maatregelen.

Het is een pakket van maatregelen dat nodig is om vertrouwelijke-, privacy-gevoelige- en/of bedrijfskritische informatie te beschermen. Additionele maatregelen worden vereist als een proces een hoog risicoprofiel heeft. Dit geldt ook bij een lager risicoprofiel van het proces in combinatie met een grote hoeveelheid aan gevoelige persoonsgegevens- en/of vertrouwelijke gegevens.

De additionele 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 de 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. Maatregelen voor naleving

Leeswijzer

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.

Actoren bij de additionele beveiligingsmaatregelen zijn medewerker, proceseigenaar, Functioneel beheerder (super user), (ICT)projectleider,Team ICT, Security Manager, Bedrijfsvoering, externe hostingleverancier,externe softwareleverancier, onderhoudsfirma, auditor

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

1. Definities

Medewerkers	in dienst van EP-Nuffic
Tijdelijk personeel	personen die worden ingehuurd
Externe medewerkers	medewerkers van externe organisaties die binnen een applicatie samenwerken met de EP-Nuffic (bijvoorbeeld ambassades, instellingen)
Klanten	personen die een dienst afnemen van de EP-Nuffic (bijv. studenten)
Beheerders	personen die de IT infrastructuur, middelen (ook niet geautomatiseerd) en/of applicaties beheren

2. Beveiligingseisen ten aanzien van personeel

2.1 AO controleren

De Proceseigenaar ziet erop toe dat de AO (operationele proces) goed wordt uitgevoerd. Via een geïntegreerde auditbenadering conform EP-Nuffic Auditplan worden de IT en de AO in samenhang beoordeeld.

Actor: Proceseigenaar
Actor: medewerker processen en systemen
Actor: (interne/externe) Auditor beoordeelt IT en de AO in samenhang
Scope: EP-Nuffic

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

3.1 Werkplek

Indien de medewerker niet bij de werkplek is (binnen of buiten kantoor) is de informatie waarmee hij werkt niet toegankelijk. In dat geval worden ladenblokken en kasten afgesloten, indien er gevoelige informatie in ligt.

Actor: medewerker
Scope: EP-Nuffic, extern

3.2 Digitale watermerken

Gevoelige digitale documenten worden bij voorkeur gewatermerkt en opgeslagen. Dit geldt o.a. voor paspoort kopieën en kopieën van andere identificatiebewijzen.

Actor: externe softwareleverancier
Scope: EP-Nuffic, extern

3.3 Gegevensdragers

De gegevensdragers met persoonsgegevens worden in een afgesloten ruimte bewaard.

Actor: medewerker
Scope: EP-Nuffic

3.4 Vernietiging gegevens

Gegevens(dragers) worden vernietigd zodra het niet meer noodzakelijk is gegevens voor een gerechtvaardigd doeleinde te bewaren. Er wordt een verklaring afgegeven dat de gegevens zijn vernietigd. Met de onderhoudsfirma en externe hostingleverancier wordt contractueel vastgelegd dat er een geheimhoudingsplicht berust op de gegevens van de EP-Nuffic. Ook wordt na beëindiging van het contract met de externe hostingleverancier, van de host een verklaring gevraagd dat de gegevens van de EP-Nuffic zijn vernietigd.

Actor: Team ICT, externe hostingleverancier, onderhoudsfirma
Actor: Functioneel beheerder voor coördineren verklaring van vernietiging en contractueel geheimhouding afspreken met onderhoudsfirma en externe hostingleverancier
Scope: EP-Nuffic, extern

3.5 Vernietigen papier

Vertrouwelijke- en persoonsgegevens (zoals beursaanvraag- en diplomawaarderingdossiers) die niet langer bewaard hoeven te blijven, worden in daarvoor bestemde beveiligde containers gedeponeerd. Een externe partij, waarmee de EP-Nuffic in overleg met de Security Manager en JZI, een contract heeft afgesloten, voert deze stukken af ter vernietiging.

Actor: medewerker

Actor: Bedrijfsvoering voor contracteren en bewaken afspraken met externe partij die papier vernietigt

Scope: EP-Nuffic

4. Maatregelen in het beheer van communicatie- en bedieningsprocessen

4.1 Vertrouwelijke- en persoonsgegevens

Vertrouwelijke en persoonsgegevens (zoals paspoortscans) mogen slechts binnen een beschermde database worden opgeslagen, verwerkt en beheerd en niet daarbuiten. Er wordt niet met gevoelige EP-Nuffic gegevens op openbare locaties gewerkt en er worden geen gevoelige EP-Nuffic gegevens op privé apparatuur opgeslagen.

Actor: medewerker
Scope: EP-Nuffic, extern

Gegevens moeten versleuteld in de databases opgeslagen worden.

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

4.2 Versleuteling externe database

Van een extern opgeslagen database dienen de actuele keys en andere ontsleutelingsinformatie beschikbaar te worden gesteld aan de Security manager.

Actor: externe hostingleverancier
Scope: extern

4.3 Geen opslag in cloud

Opslag van gevoelige gegevens in de cloud is niet toegestaan.

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

4.4 Beveiliging netwerkverkeer

Vertrouwelijke gegevens mogen enkel verzonden worden door ze tijdens de gehele transportketen over het internet te beveiligen met een actueel versleutelingalgoritme. Voor webverkeer is dit HTTPS (certificaat, TLS, minimale CSR sleutellengte van 2048 bits). Verzenden van vertrouwelijke gegevens via e-mail is niet toegestaan.
Er wordt standaard via ssllabs.com een controle gedaan op de configuratie van de webserver. Er dient tenminste een A beoordeling te worden gehaald.

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

4.5 Loggen

Bij aanpassen van gevoelige gegevens worden datum, tijdstip, gebruikersnaam en welk object gelogd.

Actor: Team ICT, externe softwareleverancier

Scope: EP-Nuffic, extern

5. Toegangsbeveiligingsmaatregelen

5.1 Controle op toegangsrechten

De Functioneel beheerder verifieert of de accounts met speciale bevoegdheden alleen aan de supervisor/beheerder zijn verleend.

De Functioneel beheerder doet een steekproef op het beheer van de autorisatiematrix om te controleren of de matrix nog altijd voldoet aan de omstandigheden van dat moment. Dit houdt in controle in de accounts of de handelingen die ermee kunnen worden uitgevoerd conform de autorisatiematrix zijn. Zo niet dient ofwel de autorisatiematrix te worden aangepast of wel dienen de bevoegdheden van een account te worden aangepast. De steekproef wordt gecommuniceerd aan de Proceseigenaar en vervolgens gearchiveerd.

Actor: Functioneel beheerder
Scope: EP-Nuffic

5.2 Wachtwoorden voor applicaties

In het algemeen gelden de volgende eisen:

- De twintig laatst gebruikte wachtwoorden mogen niet worden hergebruikt;
- De minimum wachtwoordlengte is acht tekens;
- Klanten: De wachtwoordduur is onbeperkt
- Externe medewerker dan wel medewerker: De wachtwoordduur is 6 maanden

Aanvullend geldt voor verderop uitgewerkte situaties één van de volgende wachtwoord policies:

Wachtwoord policy 1 (hierna ww1)

- Het wachtwoord dient zowel hoofd als kleine letters te bevatten.

Wachtwoord policy 2 (hierna ww2)

- Het wachtwoord dient een combinatie te zijn van tenminste drie van de onderstaande categorieën
    - hoofdletters
    - kleine letters
    - cijfers
    - symbolen

Wachtwoord policy 3 (hierna ww3)

- Het wachtwoord dient tekens te bevatten uit minimaal drie van de onderstaande categorieën.
    - hoofdletters
    - kleine letters
    - cijfers
    - symbolen
    - unicode tekens

- gerbuikersnaam mag geen onderdeel zijn van het wachtwoord.

Wachtwoordpolicies voor specifieke situaties

	Klant medewerker	**Medewerker**	**Externe**
AD account	ww1	ww3	ww3
Geen AD account	ww1	ww2	ww2

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

5.3 Aanmeldpogingen

Het aantal mislukte aanmeldpogingen wordt beperkt tot drie, waarna toegang tot het systeem volledig geblokkeerd wordt. Alleen via een vastgestelde procedure kunnen wachtwoorden worden gereset.

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

5.4 Vastleggen aanmeldpogingen

Elke poging om toegang te krijgen tot een informatiesysteem met gevoelige- en of persoonsgegevens wordt vastgelegd in een logbestand. Dit logbestand heeft een voldoende lange bewaartijd, zodat bij bijzonderheden een analyse kan worden gemaakt en hierover kan worden gerapporteerd. Mislukte aanmeldpogingen worden gevolgd en gemeld. Een proceseigenaar beslist of reactief of proactief wordt gereageerd op de logbestanden.

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

5.5 Time-out voor applicaties

Applicaties worden na 15 minuten automatisch vergrendeld om toegang door onbevoegden te voorkomen.

Actor: externe softwareleverancier
Scope: EP-Nuffic, extern

6. Beveiligingseisen voor verwerving, ontwikkeling en onderhoud van informatiesystemen

6.1 Contractuele bescherming intellectueel eigendom

Het intellectueel eigendom van data binnen applicaties wordt contractueel geregeld

Actor: (ICT)projectleider en Functioneel beheerder, externe software leverancier
Scope: EP-Nuffic

6.2 Deponering broncode

Het deponeren van broncodes is van toepassing indien het gaat om maatwerk en de EP-Nuffic geen intellectueel eigendom van applicaties heeft. Voor de verwerking van additioneel beveiligdegegevens dient de software van derden gedeponeerd te worden onder het regime van een ESCROW overeenkomst. Dit is een overeenkomst waarbij, bij een derde buiten de macht van de software ontwikkelaar, de volledige broncode wordt gedeponeerd. De broncode kan in geval van niet-nakoming van contractuele verplichtingen van de software ontwikkelaar of bij calamiteiten, binnen de contractstermen beschikbaar worden gemaakt voor de verantwoordelijke. De volledige broncode wordt per major release bijgewerkt en met een afgesproken frequentie gedeponeerd.

Actor: (ICT)projectleider en Functioneel beheerder, externe software leverancier
Scope: EP-Nuffic

6.3 Best practices product & platform

De externe softwareleverancier dient aan te kunnen tonen dat hij voldoet aan de best practices van het gebruikte product en platform.

Bij webapplicaties dient de externe softwareleverancier te kunnen aantonen dat hij voldoende maatregelen heeft genomen om de kritische web applicatie beveiligingsrisico's te beheersen (zoals aangegeven in OWASP Top 10).
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: externe softwareleverancier
Scope: extern, EP-Nuffic

6.4 Functiescheiding

Functiescheiding in AO moet 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
Scope: EP-Nuffic, extern

6.5 Geen gebruik persoonsgegevens

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

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

7. Maatregelen voor naleving

7.1 Controle beveiligingsnormen

Aan het begin van het project wordt een risicoanalyse gemaakt, en op basis hiervan bepaalt de TC Control in overleg met de opdrachtgever, de projectleider en de Security Manager van het team ICT in hoeverre een externe audit gewenst is en welke scope dan voor een dergelijke audit geldt, alsmede op welke wijze wordt geaudit. Bijvoorbeeld een soucecode review en/of penetratietest.

Actor: TC Control
Scope: EP-Nuffic, extern

De projectleider bewaakt gedurende het project dat de nodige maatregelen van het beveiligingsbeleid adequaat worden meegenomen. Indien met de TC Control afgesproken is dat een externe audit vereist is, zal de externe auditor tijdig ingeschakeld worden. Deze activiteit dient binnen het project te worden ingepland. De opdrachtgever van de externe audit is de TC Control.

Actor: projectleider
Scope: EP-Nuffic, extern

Vóór oplevering, zorgt de projectleider voor een officieel rapport waarin wordt aangegeven hoe de maatregelen van het Informatiebeveiligingsbeleid zijn geïmplementeerd (hierin is ook het resultaat van de externe audit meegenomen).

Actor: projectleider
Scope: EP-Nuffic, extern

De opdrachtgever accordeert dit rapport en geeft hiermee aan dat het systeem voldoet aan het Informatiebeveiligingsbeleid dan wel geeft deze aan de over gebleven risico's te accepteren.
Dit rapport is onderdeel van het projectdossier en kan later worden opgevraagd door o.a. de accountant, externe auditor etc.

Actor: opdrachtgever
Scope: EP-Nuffic, extern

Samen met dit rapport wordt vervolgens een wijzigingsaanvraag richting de wijzigingsbeheerder ICT ingediend met het verzoek om de wijziging in productie te nemen. De wijzigingsbeheerder van ICT controleert met de Security Manager of de resterende risico's acceptabel zijn. Indien er escalatie nodig is, zal de wijzigingsbeheerder dit richting de portefeuillehouder Bedrijfsvoering aangeven en de portefeuillehouder Bedrijfsvoering zal dan samen met de betreffende portefeuillehouder tot een besluit komen.

Actor: wijzigingsbeheerder, portefeuillehouder Bedrijfsvoering
Scope: EP-Nuffic, extern

Een auditor beoordeelt of applicaties voldoen aan het beveiligingsbeleid- en aan de additionele- en baseline maatregelen. Dit gebeurt standaard bij de oplevering, alsmede ook tijdens het beheer, omdat er wordt doorontwikkeld. De frequentie van beoordelingen is conform Auditplan EP-Nuffic.

Actor: projectleider, auditor
Scope: EP-Nuffic, extern