

Bijlage IX bij de Raamovereenkomst voor de Dienstverlening van  
Pre-employment Screening



## **Vrijwaringsverklaring**

*Inzake de uitvoering van een Penetratietest voor de aanbesteding  
Pre-employment screening*

<Opdrachtnemersnaam> en UWV

## **De ondergetekenden:**

1. Uitvoeringsinstituut werknemersverzekeringen (UWV), rechtspersoon naar de wet als bedoeld in artikel 2 Wet Structuur uitvoering werk en inkomen, gevestigd te Amsterdam, hierna te noemen: "Opdrachtgever",

en

2. <Naam te onderzoeken leverancier (s)>, gevestigd te <vestiging volgens inschrijving KvK>,) ingeschreven in het Handelsregister onder nummer [invullen] te dezen rechtsgeldig vertegenwoordigd door de heer/ mevrouw < verantwoordelijke>, Directeur < leverancier>, hierna te noemen: de Onderzochte Partij.

samen te noemen: de partijen.

## **Overwegende dat:**

- Tussen partijen is een raamovereenkomst (hierna te noemen: Hoofdovereenkomst) gesloten voor de levering van pre-employment screenings waar deze vrijwaringsverklaring een bijlage van is.
- Het beheer van <naam van de te leveren dienst/het te leveren systeem> is ondergebracht bij de Onderzochte Partij.
- UWV door middel van een zogenaamde Penetratietest een onderzoek wenst te (laten) doen naar de informatiebeveiliging binnen de door de Onderzochte Partij geleverde diensten c.q. het door Onderzochte Partij beheerde systeem.
- Het doel van de Penetratietest is om:
  1. Inzicht te krijgen in de risico's en kwetsbaarheden van de te onderzoeken diensten/systemen en te bezien of deze voldoen aan het overeengekomen beveiligingsniveau.
  2. De beveiliging van de geleverde diensten/het geleverde systeem te verbeteren.
- De in het kader van de Penetratietest door UWV te verrichten testwerkzaamheden mogelijkerwijs schade tot gevolg zouden kunnen hebben.
- De Penetratietest –onder meer gelet op het bepaalde in artikel 138ab Wetboek van Strafrecht– alleen kan geschieden met toestemming van de Onderzochte Partij.
- Dit document een beperkte vrijwaring bevat ten behoeve van UWV tegen eventuele aansprakelijkheden voor schade als gevolg van een Penetratietest .
- Partijen hun afspraken in verband met de uitvoering van de Penetratietest in deze vrijwaringsverklaring vastleggen.

## **verklaren:**

### Artikel 1 Voorwerp van de vrijwaringsverklaring

1. UWV wenst een Penetratietest uit te voeren, zoals beschreven in Bijlage I "Het Onderzoek" van deze vrijwaringsverklaring.

2. De Onderzochte Partij laat UWV vrij in de wijze waarop deze zal proberen de in Bijlage I "Het Onderzoek" beschreven computernetwerken en/of systemen binnen te dringen, dan wel in de wijze waarop gepoogd wordt gegevens aan deze computernetwerken en/of systemen te onttrekken. Dit met uitzondering van methoden waarvan het UWV op voorhand redelijkerwijs bekend moet zijn, dat die de voornoemde systemen en aangeboden diensten onbereikbaar maken, zoals denial of service-attacks. Evenmin is het UWV toegestaan om wijzigingen aan te brengen in de systemen en data die het aantreft, zodra het in de systemen is binnengedrongen.

### Artikel 2 Toestemming

1. De Onderzochte Partij geeft UWV hierbij toestemming voor het uitvoeren van een Penetratietest zoals bedoeld in het eerste lid van artikel 1.

2. De Onderzochte Partij is zich ervan bewust dat de werkzaamheden van UWV zijn gericht op het identificeren van kwetsbaarheden in de beveiliging van de geleverde diensten, het geautomatiseerde systeem, de gegevens, bedrijfsgebouwen of enig ander goed dat aan de Onderzochte Partij toebehoort of door hem wordt beheerd. Dit alles met het oogmerk om doeltreffende maatregelen te kunnen treffen ten aanzien van deze kwetsbaarheden en om, zo nodig, de beveiliging in overeenstemming te brengen met het tussen partijen overeengekomen niveau.

### Artikel 3 Uitvoering van de Penetratietest

1. UWV zal de Onderzochte Partij vooraf door middel van een aankondiging informeren over de periode waarin de Penetratietest zal plaatsvinden.

2. De Onderzochte Partij zal de ontvangst van deze aankondiging bevestigen.

3. De personen die de contacten over de uitvoering van de Penetratietest onderhouden zijn voor:

UWV : [invullen]

Onderzochte partij : [invullen]

4. De Onderzochte Partij kan UWV om gewichtige redenen met een gemotiveerd verzoek vragen een Penetratietest waarvoor toestemming is verleend te staken. UWV schort in een dergelijk geval de testwerkzaamheden op en Partijen treden in overleg. Afhankelijk van de uitkomst van het overleg zet UWV de testwerkzaamheden, al dan niet in gewijzigde vorm, voort of staakt het die werkzaamheden.

### Artikel 4 Beschikbaar stellen van onderzoeksresultaten

De resultaten van de Penetratietest worden door UWV vastgelegd in een conceptrapportage. Na afstemming van de conceptrapportage met de Onderzochte Partij, stelt UWV de rapportage definitief vast. UWV is gerechtigd de rapportage aan derden ter beschikking te stellen, waaronder auditors. UWV zal de rapportage enkel aan derden verstrekken als UWV daartoe wettelijk verplicht is of als het gaat om een externe audit, bijvoorbeeld aan SZW op grond van art. 72 Wet SUWI of aan de AP op grond van artikel 58 AVG.

Indien UWV tijdens de PEN test data, zoals gegevens van andere klanten of bedrijfsgevoelige informatie, uit de systemen van de Onderzochte Partij in handen zou krijgen, dan wordt deze data niet met derden gedeeld. Hiernaast kan deze data niet langer bewaard blijven dan noodzakelijk is voor de PEN test en wordt dit direct na afloop van het onderzoek verwijderd.

### Artikel 5 Aansprakelijkheid

1. In afwijking van de voorwaarden met betrekking tot aansprakelijkheid die gelden tussen partijen op basis van de Hoofdovereenkomst, geldt dat UWV niet aansprakelijk is voor schade die ontstaat als gevolg van diens werkzaamheden op grond van de Penetratietest, indien en voor zover deze werkzaamheden vallen binnen de reikwijdte van Bijlage I "het Onderzoek" en de desbetreffende werkzaamheden ook overigens zijn verricht conform het bepaalde in deze vrijwaringsverklaring. De Onderzochte Partij vrijwaart UWV dan ook tegen aansprakelijkheden dienaangaande, met name ingeval een derde UWV zou aanspreken wegens schending van een of meer van de artikelen 161sexies, 161septies, 351, 351bis, 138ab en 138b van het Wetboek van Strafrecht en voor zover dit niet in strijd is met de wet.

2. Voor zover UWV wel aansprakelijk is, is de hoogte van de aansprakelijkheid beperkt tot het bedrag zoals dat is overeengekomen in de tussen partijen gesloten Hoofdovereenkomst.

#### Artikel 6 Beperking vrijwaring

De vrijwaring als omschreven in artikel 5 ziet niet op schade die is ontstaan door een toerekenbare tekortkoming bij het uitvoeren van de Penetratietest door UWV dan wel bij opzet, bewuste roekeloosheid of een ernstige beroepsfout van UWV.

#### Artikel 7 Looptijd

Deze vrijwaringsverklaring treedt in werking op het moment van ondertekening door alle partijen en duurt voort totdat de tussen partijen gesloten Hoofdovereenkomst eindigt.

Aldus op de laatste van de 2 hierna genoemde data in tweevoud ondertekend:

Namens UWV, genoemd onder 1,

Naam : [invullen]

Functie : [invullen]

Datum : [invullen]

Plaats : [invullen]

Namens de Onderzochte Partij, genoemd onder 2,

Naam : [invullen]

Functie : [invullen]

Datum : [invullen]

Plaats : [invullen]

CONCEPT

## **Bijlage I "het Onderzoek"**

**Het onderzoek zal plaats vinden in de periode van X t/m X. De uitvoering zal gedaan worden door de pentesters van het UWV SOC.**

### **In scope zijnde van dit onderzoek is:**

- De webapplicatie die wordt aangeboden op het domein X (IP adres X)
- De mogelijke API end points die betrokken zijn bij de werking van de applicatie. Deze host worden automatisch in scope geplaatst ook al zijn deze op een andere IP adres te benaderen dan eerder is aangegeven.
- In het algemeen wordt onderzoek gedaan naar mogelijke security issues. Hierbij te denken aan problemen die zijn terug te vinden binnen het SSD-normen kader en / of de OWAPS webapplicatie richtlijnen.
- Onder andere wordt onderzoeken gedaan naar:
  - Het verkrijgen van data die normaal niet toegankelijk mag zijn, bijvoorbeeld die van andere gebruikers.
  - Het verkrijgen van verhoogde rechten binnen de webapplicatie.
  - Het verkrijgen van toegang tot andere gebruikersaccount of administratieve privileges/accounts door fouten in de applicatie logica.
- Het uitvoeren van een poort scan op alle betrokken hosts.
- Indien andere poorten openstaan op de hosts waar de applicatie en / of mogelijk API end points draaien dan nodig zijn voor het functioneren van de applicatie, deze verder te onderzoeken.
- Het uitvoeren van exploits op de webserver of onderliggende OS laag.

### **NIET in scope zijnde van dit onderzoek is:**

- Uitvoeren van DOS of DDOS aanvallen om de continuïteit/ beschikbaarheid te onderzoeken.
- Social engineering of andere phishing activiteiten.
- Uitvoeren van grootschalig brute force aanvallen (>100000 verzoeken op een functies in de applicatie of een URL om middels brute force toegang te krijgen tot specifieke gegevens).