

# VRIJWARINGSVERKLARING

## VULNERABILITY SCANNING

Doel van de vulnerability scanning is het onderzoeken en rapporteren van eventuele zwakheden in de (systeem)software van de internetsite of host (zoals een IP adres of URL) (hierna gezamenlijk: de “Doelen”) die gescand zullen worden. U stemt namens uw bedrijf / organisatie er mee in dat uw IT partner die deze scan(s) aanbiedt de scan(s) mag uitvoeren en u bevoegd bent om uw bedrijf / organisatie te vertegenwoordigen.

## ARTIKEL 1. ALGEMEEN

Uw IT partner spant zich naar beste kunnen in voor een zorgvuldige uitvoering van de vulnerability scans (hierna: “de Diensten”), zonder nadelige gevolgen voor de bestaande infrastructuur. Ook streeft uw IT Partner naar een goede toegankelijkheid van de website en van de door haar langs elektronische weg aangeboden Diensten. Uw IT Partner spant zich er naar beste kunnen voor in om geen (distributed) Denial of Service aanvallen uit te (laten) voeren, systemen opnieuw op te starten of enige andere activiteit te verrichten die de werking van de website of host zal verstoren en de gegevens zullen in beginsel alleen aan u worden doorgegeven en niet worden openbaar gemaakt. Indien mogelijk zullen gegevens worden verzameld voor analyse doeleinden.

De informatie verstrekt door uw IT Partner is alleen bedoeld voor algemeen gebruik en bewerkstelligt geen advies. Uw IT Partner zal niet aansprakelijk worden gesteld voor enige vorm van schade die voortvloeit uit het gebruik (of de onmogelijkheid van gebruik) van de informatie die wordt verstrekt via de website en/of de Diensten, waaronder inbegrepen schade veroorzaakt door onvolledigheid of onjuistheid van de informatie, tenzij de schade het gevolg is van opzet of bewuste roekeloosheid.

U gaat ermee akkoord dat alle uitkomsten (ook wel: de constatering of wel/geen sprake is van een inbreuk(en) op de beveiliging) die door uw IT Partner in het kader van de met u gesloten overeenkomst worden geleverd slechts hulpmiddelen zijn voor een oplossing en dat het gebruik van de Diensten assistentie van getrainde medewerkers vereist. U erkent voorts en gaat ermee akkoord dat uw IT Partner haar Diensten niet heeft voorgesteld om beveiligingsinbreuken en/of -gebreken als zodanig te verhelpen, een oplossing voor te schrijven, of andere taken te verrichten die onder het herstel van beveiligingsinbreuken en/of -gebreken vallen.

U erkent en verklaart dat:

- (i) Uw IT Partner geen controle heeft over uw beveiligingsoplossingen en over het gebruik daarvan door u; en
- (ii) Uw IT Partner niet op de hoogte is van de specifieke of unieke omstandigheden waarin de beveiligingsoplossingen door u worden gebruikt. Uw IT Partner biedt geen garantie met betrekking tot de aard of de kwaliteit van de opvolging door u naar aanleiding van de uitkomsten van de Diensten. Mochten er desondanks onjuistheden voorkomen in de uitvoering, dan aanvaardt uw IT Partner geen enkele andere aansprakelijkheid voor de eventuele gevolgen daarvan anders dan zoals bepaald in de gebruiksvoorwaarden behorende bij de Diensten.

## ARTIKEL 2. MACHTIGINGEN EN GARANTIES

- (i) U verleent aan uw IT Partner hierbij voor de duur en de uitvoering van de gesloten overeenkomst een onbeperkte toestemming tot het betreden, gebruiken en bedienen van de Doelen, inclusief alle voorliggende en bijbehorende systemen en infrastructuren, ongeacht of deze van derden zijn. U verklaart toestemming te hebben van derden die mogelijk gevolgen kunnen ondervinden van de vulnerability scans en hen naar behoren te hebben geïnformeerd over de Diensten;
- (ii) U verleent aan uw IT Partner het recht om iedere getroffen beveiligingsmaatregel aanwezig in of bij de Doelen uit te schakelen of te omzeilen en het recht de op een Doel aanwezige data te openen en te kopiëren, doch alleen indien dit noodzakelijk is voor een correcte uitvoering van de Diensten.
- (iii) U verklaart en staat er voor in dat u bevoegd bent om de in dit artikel genoemde rechten en toestemming te verlenen aan uw IT Partner. U verklaart daarnaast ook bevoegd te zijn dit recht te verlenen voor, en de toestemming te hebben van, derden die mogelijk gevolgen ondervindt als gevolg van de Diensten.

## ARTIKEL 3. AANSPRAKELIJKHEID

- (i) U zal uw IT Partner vrijwaren van alle claims en aanspraken van derden en door derden genomen juridische stappen die worden genomen in verband met de Diensten.
- (ii) Indien uw IT Partner door autoriteiten boetes worden opgelegd in verband met de werkzaamheden onder deze vrijwaringsverklaring, of de rechter een verplichting tot schadevergoeding aan een derde oplegt, dan zal u deze boetes of schadevergoeding integraal vergoeden.
- (iii) Indien medewerkers van uw IT Partner worden aangehouden, worden opgehouden of ingesloten door de politie, andere autoriteiten of privaat veiligheidspersoneel op grond van enige verdenking van strafbaar of

onrechtmatig handelen met betrekking tot de Diensten, met betrekking tot deze opdracht van u, dan bent u verplicht alles in het werk te stellen om hieraan zo snel mogelijk een einde te maken.

- (iv) Alle juridische kosten (zoals kosten van advocaten of deskundigen) die uw IT Partner moet maken in verband met een juridische claim of aanspraak in verband met de Diensten, met betrekking tot deze opdracht van u, zal door u onverwijld en volledig worden gecompenseerd. Voorwaarde is dat uw IT Partner zo snel mogelijk, indien haalbaar vooraf, meldt dat er kosten worden gemaakt en u hierbij betreft. Bovenstaande bepalingen gelden uitsluitend indien de grondslag te herleiden is tot werkzaamheden van uw IT Partner in verband met de Diensten.
- (v) De in deze vrijwaringsverklaring genoemde aansprakelijkheidsbeperkingen komen echter te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van uw IT Partner.