



Den Haag

IV eisen bij inkoop

Datum: 13-7-2020

Versie: 1.0

Status: Definitief
Vertrouwelijk

Documentnaam	IV eisen bij inkoop
Versienummer	1.0
Classificatie	Openbaar
Status	Definitief
Documenteigenaar	Jeroen Schipper
Vastgesteld door	WG IV
Vaststellingsdatum	13-7-2020
Herbeoordelingsdatum	2 jaar na vaststellingsdatum

Inhoud

Informatieveiligheidseisen/vragen bij aanbesteding en Inkoop IT 3

1. De laatste versie van de Gemeentelijke inkoopvoorwaarden bij IT (GIBIT) is van toepassing .. 3
2. Aangeven aan welk normenstel wordt voldaan 3
3. Aantonen hoe er aan het normenstelsel wordt voldaan 3
4. Jaarlijkse verantwoording ISMS..... 5
5. Aanvullende vragen 5
6. Medewerking aan het jaarlijks Hack The Hague event 5
7. Medewerking aan opname detectieportaal..... 5
8. Logging..... 5

Toelichting informatieveiligheidseisen/vragen bij aanbesteding en Inkoop IT voor de ISOFout!
Bladwijzer niet gedefinieerd.

Informatieveiligheidseisen/vragen bij aanbesteding en Inkoop IT

Onderdelen van dit gedeelte van het document worden gedeeld met de projectleiders/adviseurs/inkoop zodat deze eisen/vragen opgenomen kunnen worden in de aanbestedings of uitvraag documenten, zie ook de teksten in het rood die per situatie beoordeeld moeten worden.

Informatieveiligheidseisen

Inschrijver dient deze vragen te beantwoorden op max 1-A4.

Ten aanzien van informatieveiligheid is op de dienstverlening door een inschrijver van toepassing:

1. De laatste versie van de Gemeentelijke inkoopvoorwaarden bij IT (GIBIT) is van toepassing.
Indien nog niet eerder opgenomen in een Programma van Eisen of in de aanbestedingsstukken genoemd.
2. Aangeven aan welk normenstel wordt voldaan.
Inschrijver dient aan te geven op basis van welk normenstelsel de informatiebeveiliging plaatsvindt. Er dient een keuze gemaakt te worden uit a, b of c.

De informatiebeveiliging vindt plaats volgens:

- A. ☐ Algemeen erkende normen, namelijk:

.....
(vermeld normenstelsel, zoals bijvoorbeeld NEN7510 bij zorgverleners, NEN/ISO 27001, PCI/DSS).

- B. ☐ De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIO de BIR of vergelijkbaar, namelijk:

-
C. ☐ Anders, nl.

-
3. Aantonen hoe er aan het normenstelsel wordt voldaan.

Inschrijver dient de toereikendheid van de informatiebeveiliging, zoals opgegeven in bovenstaande eis, aan te tonen door één van de volgende certificeringen en eventueel bijbehorende verklaring van toepasselikheden. Er dient een keuze gemaakt te worden uit a, b of c.

- A. ☐ Periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
- B. ☐ Een Assurance rapport van een auditor die is aangesloten bij NOREA;
- C. ☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen, zoals hieronder beschreven (*)

.....
(*) Indien leverancier Informatieveiligheid wil aantonen met eigen controles of eigen mededelingen dan kan er een toets plaatsvinden aan de hand van de vragenlijst

“Informatieveiligheidseisen externe dienstverlening” welke de gemeente Den Haag hanteert en voor een groot deel is gebaseerd op de maatregelen uit de BIO/ISO27002.

4. Jaarlijkse verantwoording Informatieveiligheid.

De toepassing wordt jaarlijks getoetst op de implementatie van de Baseline Informatiebeveiliging Overheid (BIO), de inschrijver dient daar jaarlijks zijn medewerking aan te verlenen door vragen (vanuit de applicatie Recourse of per reguliere mail) te beantwoorden en daar waar nodig bewijs voor aan te leveren.

5. Aanvullende vragen.

Naast het feit dat de inschrijver aan moet geven en aan moet tonen aan welke normenkaders op het gebied van Informatieveiligheid wordt voldaan, moeten de onderstaande open vragen in een apart document beantwoord en daar waar nodig met bewijsstukken aangetoond worden:

- a. Worden de componenten van uw netwerk gehardened?
Denk aan besturingssystemen kritieke componenten, webserver, netwerkkapparatuur, databases)
- b. De vernietiging van opslag aan einde van het contract vindt op zodanige wijze plaats dat de gegevens met geen enkele forensische procedure kunnen worden hersteld?

6. Medewerking aan het jaarlijks Hack The Hague event.

Inschrijver is deelnemer van jaarlijks evenement Hack the Hague, stelt oplossing beschikbaar voor penetratie test tijdens evenement en zorgt voor opvolging van gevonden kwetsbaarheden tijdens het evenement.

De gemeente Den Haag organiseert jaarlijks een Hackevent. Tijdens dit event krijgen een groot aantal ethische hackers de mogelijkheid om de door de gemeente Den Haag gebruikte applicaties en systemen welke bereikbaar zijn vanaf het internet te onderwerpen aan een test. De bevindingen worden gedeeld met de leveranciers die daarna de bevinding(en) kan oplossen. Medewerking van de leverancier (beschikbaar stellen test of productie omgeving en oplossen van de kwetsbaarheden tijdens het event) wordt zeer op prijs gesteld. Echter zal er geen vergoeding tegenover staan maar kan dit in feite wel worden gezien als een meervoudige en goedkope pentest. Uiteraard zijn de deelnemende ethische hackers gebonden aan de voorwaarden van de gemeente Den Haag en hun leveranciers.

Dit artikel opnemen bij het aanbieden van de toepassing middels een webportaal/website.

7. Medewerking aan opname detectieportaal.

Inschrijver dient aan te geven of deze medewerking verleend aan het opnemen van de website(s) in een detectie portaal.

Om eventuele kwetsbaarheden van een website in een zo vroeg mogelijk stadium te detecteren maakt de gemeente Den Haag gebruik van Cybersprint.

Het door Cybersprint gebruikte Digital Risk Protection platform detecteert automatisch alle online kwetsbaarheden van bekende, 'verborgen', en valse online toegangspunten. Zij brengen het online aanvalsvlak in beeld en geven advies over mogelijke maatregelen. De door gemeente Den Haag gebruikte website zal, indien leverancier hiermee instemt, opgenomen worden in het Cybersprint portaal waarna er bij het ontdekken van kwetsbaarheden bevindingen doorgegeven zullen worden en na en redelijke termijn opgelost moeten worden.

Dit artikel opnemen bij het aanbieden van de toepassing middels een webportaal/website.

8. Logging

De applicatie wordt ingericht conform de relevante eisen t.a.v. logging vanuit de AVG en/of BRP.