Technisch website beleid H2O

- Beveiligingsbeleid
- Toegankelijkheidsbeleid
- Archivering
- Beheer

Versie: 1.7 (aangepast n.a.v. vraag NVI 1)
Datum: 13-09-2022

Auteurs	Advies gevraagd aan
Amber Schutteman	Hans Hendriks
Anthe Oosterveld	Jeroen van Eikenhorst
Chantal Lokate	Marja Vink
Dolf van Warven	
Edwin de Vries	
Radjen Santram	

Inhoudsopgave

1 Inleiding

Aan overheidswebsites worden (wettelijke) eisen gesteld. In de afgelopen jaren zijn er meer en aanvullende richtlijnen gekomen voor overheidswebsites. Dit maakt het noodzakelijk om hier duidelijke afspraken over vast te leggen, die gebruikt kunnen worden bij de toetsing van de huidige en toekomstige websites. Onder overheidswebsites verstaan wij naast websites ook dienstverleningsportalen zoals bijvoorbeeld de afsprakenmodule en burgerportaal voor Burgerzaken.

Doel van dit document is dan ook het vaststellen en vastleggen waar onze gemeentelijke websites aan dienen te voldoen. In de basis gaat het om de volgende vier hoofdonderdelen (BTAB):

- **B**eveiligingsbeleid
- **T**oegankelijkheidsbeleid
- **A**rchivering
- **B**eheer

In dit document wordt uitsluitend gesproken over de eisen aan websites als communicatiemiddel en waar je dan met name vanuit de wetgeving van de overheid rekening mee moet houden. We gaan in dit document niet in op de eisen waar de inhoud van een website aan moet voldoen of wanneer het opzetten van een website gerechtvaardigd is. Dat wordt opgenomen in een nog op te stellen 'visie op digitale kanalen'.

In de hierna volgende hoofdstukken worden de bovengenoemde hoofdonderdelen nader toegelicht en voorzien van een overzicht per onderwerp waar de websites op dat onderdeel aan moeten voldoen.

Team communicatie, de informatieadviseurs en afdeling DIV adviseren over de punten genoemd in dit websitebeleid. Elke website moet (gaan) voldoen aan de eisen gesteld in dit plan.

1.1 Gemeentelijke website

Een gemeentelijke website heeft een of meer van de volgende kenmerken:

- De gemeente is domeinnaamhouder[1]
- De website gebruikt de huisstijl van de gemeente
- De website is (mede) door de gemeente geïnitieerd
- De website is (mede) door de gemeente gefinancierd / gesubsidieerd
- De website wordt door de gemeente onderhouden
- De website wordt door inwoners als zodanig beschouwd
- De website is onderdeel van een samenwerkingsverband tussen gemeenten en/of bedrijven

[1] Alleen de domeinnaamhouder kan een PKI-overheid certificaat aanvragen.

2 Beveiligingsbeleid websites

2.1 Ontwikkeling

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van inwoners, bedrijven, medewerkers en ketenpartners voor gemeenten van groot belang. Het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan grote gevolgen hebben. Denk daarbij aan identiteitsfraude, privacy schending of een gehackte website. De gemeente loopt hier kans op imagoschade en/of financiële schade. Een betrouwbare en veilige informatiehuishouding is dan ook essentieel voor de (digitale) dienstverlening van gemeenten.

Dit betekent voor de websites van de gemeente, dat deze moeten worden voorzien van beveiligingscertificaten, moeten voldoen aan internetstandaarden en regelmatig gescand/ gepentest moeten worden om eventuele kwetsbaarheden aan het licht te brengen. In de hierna volgende paragrafen worden deze onderwerpen nader toegelicht. Daarna volgt een overzicht van gedefinieerde betrouwbaarheidsniveaus op basis van het classificatiemodel van de handreiking Betrouwbaarheidsniveaus voor digitale dienstverlening[2]. Dit model is vertaald naar de situatie van Hattem, Heerde en Oldebroek.

2.2 Beveiligingscertificaat

Beveiligingscertificaten zijn een onmisbare schakel in beveiligd internetverkeer. Een certificaat is een legitimatiebewijs van een website of ICT-systeem. Daarnaast bevat het gegevens die nodig zijn voor beveiligd internetverkeer. Google en andere leveranciers van webbrowsers bestempelen websites zonder certificaat standaard als onveilig en waarschuwen de gebruiker hier ook voor. Certificaten zijn er in vele soorten en maten. De keuze voor een certificaat is afhankelijk van de mate van beveiliging die benodigd is.

Het Forum Standaardisatie (Logius) adviseert voor overheidswebsites om altijd gebruik te maken van PKI-overheid certificaten. Een PKI-overheid certificaat waarborgt de betrouwbaarheid van informatie-uitwisseling via e-mail en websites op basis van Nederlandse wetgeving en is de internationale standaard voor het beveiligen van gegevens en berichten.

Voordelen PKI-overheid-certificaat:

- Exclusief keurmerk van de Staat der Nederlanden.
- Gebaseerd op Nederlandse wet- en regelgeving en Europese standaarden.
- Beheer van de standaard door de Rijksoverheid. Regie van incidenten of calamiteiten door de Rijksoverheid.
- Actief toezicht op de certificatiedienstverleners door de Rijksoverheid.
- Veilig imago als gevolg van de hoge beveiligingsnorm van PKI-overheid t.o.v. Commodo certificaten
- Het PKI-overheid certificaat is de standaard voor het beveiligen van elektronische communicatie door en met de overheid.
- Het gebruik van de Certificate Revocation List (CRL) is een lijst met certificaat serienummers die herroepen zijn, niet meer geldig zijn en niet meer te vertrouwen zijn voor gebruikers.[3]

[2] https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus

[3] Een CRL wordt periodiek gemaakt. De CRL wordt altijd uitgegeven (vaak elke 24 uur) door een Certificate Authority (CA) die zich alleen toespitst op hun eigen certificaten. Alle CRL's hebben een (vaak korte) periode waarin ze geldig zijn. Deze CRL's kunnen worden geraadpleegd door applicaties met PKI functionaliteit. Om spoofing of denial-of-service aanvallen te voorkomen zijn CRL's vaak digitaal ondertekend door de CA van de CRL.

Een PKI-overheid certificaat beveiligt de verbinding en garandeert dat je daadwerkelijk verbinding maakt met het domein dat in de adresbalk te zien is.
In een aantal gevallen volstaat het om een lichter SSL certificaat te gebruiken. Dit is afhankelijk van het betrouwbaarheidsniveau.

Indien er gesproken wordt over een lichter SSL certificaat, dan gaat het over een certificaat met de volgende vereisten:

- Xolphin SSL Beveiligingscertificaat met organisatievalidatie.
- UTN/AddTrust rootcertificaat, vertrouwt door alle moderne (mobiele browsers en applicaties, voorkomt foutmeldingen en waarschuwingen.
- Standaard SHA-256 certificaat op basis van RSA (dit is tevens ook de standaard voor PKI-Overheid certificaat)

Verder geldt voor het gebruik van alle officiële certificaten (PKI en lichtere SSL-certificaat), dat deze herkenbaar zijn aan een groen slotje in de adresbalk (URL).
Voor het aanvragen van een certificaat is het van belang, dat de gemeente eigenaar is van de domeinnaam.

2.3 Internetstandaarden

Internetstandaarden maken het mogelijk dat computers wereldwijd gegevens kunnen uitwisselen. Overheden zijn verplicht hiervoor de open standaarden te implementeren en te hanteren. Deze zijn vastgesteld door het Forum Standaardisatie (onderdeel van Logius) (https://www.forumstandaardisatie.nl) en staan beschreven op de lijst met 'pas toe of leg uit'-standaarden. Iedere website (en of geïmplementeerde CMS-omgeving) moet daarom voldoen aan de moderne internetstandaarden (incl. gebruik TLS 1.2, SPF, DKIM, DMARC, DNSSEC, STARTTLS, DANE en IPV6, HTTPS en HSTS verkeer).

Enkele voorbeelden van toepassing van moderne internetstandaarden:

- IPv6 Internet Protocol v6, als dit niet wordt ondersteund door de hostingprovider dan is de website niet bereikbaar voor bezoekers met een modern (IPv6) internetadres.
- DNSSEC: DNSSEC beschermt bezoekers (die controle van domein-handtekeningen geactiveerd hebben) tegen gemanipuleerde vertaling van de domeinnaam naar kwaadaardige internetadressen.
- HTTPS: HTTPS is het beveiligen van de verbinding, beschermd tegen afluisteren en manipulatie.

Toetsen of een website voldoet aan de moderne internetstandaarden kan op verschillende manieren. Vooraf moet een website natuurlijk al voldoen, maar eenmaal live moet een website ook blijven voldoen. Op www.internet.nl (een initiatief van onder meer de Nederlandse overheid) zie je of een website voldoet aan de belangrijkste internetstandaarden. Hiermee voldoen we tevens aan de verplichte open standaarden zoals opgesteld door het Forum standaardisatie (eis uit de Baseline Informatiebeveiliging Overheid). Daarbij geldt dat qua beveiliging (o.a. juist gebruik van certificaten) de oplossing een rating bij SSLLabs.com dient te hebben van minimaal een A+.

2.4 Scannen en pentesten

Om kwaadwillenden voor te zijn is het belangrijk om, met behulp van. een scantool (bijvoorbeeld ‘Qualys vulnerability management’), websites structureel te scannen op kwetsbaarheden. Een pentest of penetratietest gaat wat verder, dit is een test c.q. poging tot hacken, waarbij geprobeerd wordt in te breken op een systeem om zo mogelijke kwetsbaarheden boven water te krijgen. Een dergelijke test zal door een gespecialiseerd bedrijf moeten worden uitgevoerd. Frequentie van scannen en of een site gepentest wordt, is afhankelijk van het betrouwbaarheidsniveau (zie 2.11.1).

Iedere DigiD toepassing op een website (Frontoffice CMS en iBurgerzaken) moet worden ge-audit. Na een positief oordeel van de auditor wordt jaarlijks door Logius goedkeuring verleend en mag de DigiD-koppeling weer een jaar worden gebruikt . Daarnaast is een TPM-verklaring van de leverancier (Norm ICT-beveiligingsassessments DigiD versie 2.0' van Logius), standaard onderdeel van de jaarlijkse ENSIA verantwoording.

2.5 Versies en versiebeheer browsers en CMS

De website functioneert minstens in de laatste twee versies van de door de gemeenten ondersteunde browsers (Microsoft Edge, Google Chrome, Apple Safari en Mozilla Firefox) zonder gebruik te maken van plug-ins (zoals Java, Flash, Silverlight, ActiveX, etc.). De websites moeten daarbij het gebruik van tablets, smartphones en andere mobiele devices ondersteunen via aangepaste interface of responsive design zonder kwaliteit in te leveren op leesbaarheid van tekst en met behoud van alle functionaliteiten. Dit laatste binnen de mogelijkheden/beperkingen die het specifieke device hiervoor heeft.

De meeste websites draaien tegenwoordig op zogenaamde content management systemen (CMS) en het is zaak deze systemen up-to-date te houden. Het blijven gebruiken van een oudere versie maakt de website kwetsbaar voor cyberaanvallen. Leveranciers van CMS systemen brengen om de zoveel jaar of zelfs maandelijks een nieuwe versie uit. Het is noodzakelijk om de updates tijdig uit te voeren in verband met de veiligheid van de websites. Dit geldt overigens voor het geheel aan infrastructuur, dus ook voor de eventuele achterliggende DMS omgeving, maar ook het operating systeem waar het CMS op draait. Daarbij worden de updates/wijzigingen eerst getest in de CMS testomgeving en de koppeling met de DMS/Zaaksysteem (ZS) testomgeving wordt getest.

Als vereiste kan worden gesteld dat de leverancier van het CMS systeem waarborgt dat de aangeboden Oplossing niet meer dan één major versie achterloopt ('neerwaartse compatibiliteit') op de open standaarden van het Forum Standaardisatie die voor de Oplossing van toepassing zijn. Aanpassingen in de standaarden worden door de leverancier verwerkt binnen 12 maanden nadat deze niet meer door Forum Standaardisatie als geldende standaard worden ondersteund. Daarnaast wordt de oude versie van de standaard nog minimaal 12 maanden ondersteund.

2.6 Wachtwoorden

2.6.1 Beheer

Een sterk wachtwoord helpt bij het voorkomen van ongewenste toegang tot systemen, dit is bij CMS systemen niet anders. Eisen aan het functioneel beheerders wachtwoord: minimaal 10 karakters 1 hoofdletter, 1 cijfer, 1 speciaal teken, geen generiek account, halfjaarlijks verversen. Eisen moeten worden afgedwongen door de software. Deze eis is afkomstig uit het Logische Toegangsbeveiligingsbeleid van de H2O-gemeenten. Verder gelden voor beheer de algemene beheerafspraken en standaarden voor het uitvoeren van de beheertaken.

2.6.2 Gebruikers

Voor de gebruikers van websites gelden andere eisen. Zo zijn er al specifieke regels vastgesteld bij gebruik van DigiD, eiDas, e-Herkenning. Voor de eisen aan deze onderdelen wordt verwezen naar de landelijke regelgeving voor deze componenten (zie hiervoor onder meer: https://www.digitaleoverheid.nl/dossiers/wet-digitale-overheid/). Voor een eenvoudige login-functie (bijvoorbeeld aan/afmelden nieuwsbrief) gelden de eisen: minimaal 8 karakters 1 hoofdletter, 1 kleine letter, 1 cijfer, 1 speciaal teken. Eisen moeten worden afgedwongen door de software. Deze eis is afkomstig uit het Logische Toegangsbeveiligingsbeleid.

2.7 Privacy

2.7.1 Privacyverklaring

Als een website privacygevoelige (persoons)gegevens verwerkt (verzamelt, bewerkt en/of opslaat), bijvoorbeeld via een online formulier, is het verplicht een privacyverklaring op te stellen. In de privacyverklaring moet zo duidelijk mogelijk worden omschreven voor welke doeleinden de verwerkingsverantwoordelijke de verzamelde gegevens gaat gebruiken. De privacyverklaring bevat minimaal: naam en contactgegevens van de organisatie, wettelijke grondslag, wie de persoonsgegevens krijgt, of er doorgifte is buiten de EER, hoelang we de gegevens bewaren, de rechten van de betrokkenen, waar je een klacht kan indienen, wordt er gebruik gemaakt van geautomatiseerde besluitvorming, is het verplicht om de persoonsgegevens aan te leveren en zo ja waarom.

2.7.2 Cookieverklaring

Cookies zijn kleine tekstbestanden die een website op je computer, tablet of mobiele telefoon plaatst op het moment dat je de website bezoekt. In deze cookies wordt informatie over een websitebezoek opgeslagen. Cookies worden vaak onderverdeeld in de volgende drie categorieën (functioneel, analytische en tracking).

1. Functionele cookies: Functionele cookies zijn nodig om de website gebruikersvriendelijk te maken voor de bezoeker.
2. Analytische cookies. Websites plaatsen analytische cookies om te meten hoe vaak een website wordt bezocht.
3. Tracking cookies van derden.

Het moet bij elke website duidelijk zijn welke cookies worden gebruikt en dit moet op de website worden opgenomen. Voor sommige cookies moet toestemming worden gevraagd aan de gebruiker door middel van een cookiemelding.

Soorten cookies	Toestemming vragen
Functionele cookies	Nee
Analytische cookies	Nee*
Tracking cookies van derden	Ja

* Mits cookies alleen gebruikt worden om bezoekers te tellen, om zo inzicht te krijgen in het functioneren van de website. Het is in dit geval wel verplicht om websitebezoekers te informeren over het plaatsen van deze cookies.

2.7.3 Verwerkersovereenkomst

Om tot afspraken te komen over de verwerking van persoonsgegevens maken we gebruik van de meest recente versie van de standaard verwerkersovereenkomst van VNG. Deze standaard wordt gebruikt als aanvulling op een hoofdovereenkomst om op grond van de AVG (artikel 28.3 en 28.9) nadere afspraken te maken en vast te leggen over de omgang met persoonsgegevens.

De meest recente versie van de standaard verwerkersovereenkomst VNG is beschikbaar via de website van de VNG of neem contact op met de Privacy Officer of Functionaris Gegevensbescherming.

2.8 Contract en SLA

Er dient een contract / Service Level Agreement (SLA) te zijn met de leverancier van de website met daarin afspraken over onder andere beschikbaarheid en ondersteuning. Het contract moet voldoen

aan de actueel geldende GIBIT voorwaarden[4] en in een SLA moet minimaal het volgende worden opgenomen:

1. Dienstenniveau:
2. Openingstijden;
   a. bereikbaarheid;
   b. prioritering incidenten;
   c. reactietijd van de incidentmelding;
   d. afhandeling, responstijden en hersteltermijnen;
   e. escalatieprocedure.
3. Back-up-, recovery- en uitwijkprocedure
   a. Eventuele aanvullende ISO normen waaraan voldaan kan worden.
4. Monitoring applicatie en connectiviteit.
5. Eigendom van data.
6. Beveiligingsmaatregelen
7. Exit strategie (invulling artikel 22 GIBIT 2020):
   a. Teruggave data (wijze, format, termijn);
   b. Kosten transport data, conversie en migratie naar een andere cloud leverancier of naar interne IT-omgeving;
   c. Bestandsformaat
   d. Vernietiging data
   e. Termijn van teruggave en vernietiging.
8. Beschikbaarheidsgarantie. Uptime. Downtime.
9. Continuïteitsgarantie (conform artikel 30 GIBIT 2020): beschrijving hoe continuïteit is geborgd.
10. Wijziging van dienst.
11. Beschrijving procedure Testen software en ingebruikname.
12. Incidentafhandeling: Leverancier heeft incidentbeheer geïmplementeerd voor detecteren van incidenten, de schade ervan te beperken en de klanten hierover te informeren.
13. Patches/verbeteringen/ aanpassingen/updates/upgrades en onderhoud
14. Looptijd (gelijk aan looptijd hoofdovereenkomst).
15. Audits. Uitvoeren/toestaan van in- en externe audits conform artikel 21.6 GIBIT 2020.

2.9 Tools / applicaties

Op websites wordt vaak gebruik gemaakt van verschillende tools/ applicaties /formulieren. Deze worden vaak gebruikt voor onder andere enquêtes en aanmelding voor nieuwsbrieven. Ook daar zijn een aantal voorwaarden voor opgesteld.

2.9.1 Online formulieren

Voor online formulieren geldt dat er gebruik gemaakt moet worden van de formulierenvoorziening van de leverancier van de betreffende website zelf of de gemeentelijke preferred supplier van formulieren (huidige online formulieren H2O: Roxit/GreenValley). Dus niet van een buitenstaande derde partij, waar geen overeenkomst mee gesloten kan worden. Het gebruik is afhankelijk van het betrouwbaarheidsniveau (zie 2.11.1).

Eisen aan formulierenvoorziening:

- Verwerkersovereenkomst met leverancier
- PKI-overheid certificaat, soort afhankelijk van betrouwbaarheidsniveau, (zie 2.11.1).
- Beveiligde koppelingen moeten voldoen aan de moderne internetstandaarden conform de open standaarden van Forum Standaardisatie (https://www.forumstandaardisatie.nl).

[4] De actueel geldende GIBIT-voorwaarden zijn op te vragen bij de afdeling Inkoop

Beveiligde emailvoorziening bij voorkeur via een koppeling met onze eigen beveiligde mailvoorziening (Zivver)
- De meest recente toegankelijkheidseisen (WCAG)
- Opslag/doorgifte persoonsgegevens op servers binnen de EER (onderdeel van de verwerkersovereenkomst)
- Privacyverklaring
- Formulieren moeten voldoen aan privacy by default en privacy by design (zie 2.10.

2.9.2 Nieuwsbrieven functionaliteit

Voor nieuwsbrieven geldt dat er gebruik gemaakt moet worden van de nieuwsbrief functionaliteit van de leverancier van de betreffende website of de gemeentelijke preferred supplier van nieuwsbrieven (die momenteel nog niet aanwezig is). Dus niet van een buitenstaande derde partij, waar geen overeenkomst mee gesloten kan worden. Het gebruik is afhankelijk van betrouwbaarheidsniveau (zie 2.11.1).

Eisen aan nieuwsbrief functionaliteit:

- Toestemming vragen aan gebruiker en informeren via privacyverklaring
- Voldoen aan de moderne internetstandaarden conform open standaarden van Forum Standaardisatie
- Opt-in en opt-out mogelijkheid is vereist
- Verwerkersovereenkomst met (diensten) leverancier
- Beveiligde emailvoorziening zie 2.9.1
- De meest recente toegankelijkheidseisen (WCAG)
- Opslag/doorgifte persoonsgegevens op servers binnen de EER (onderdeel van de verwerkersovereenkomst)

2.9.3 Enquête/survey functionaliteit

Voor een enquête/survey functionaliteit geldt dat er gebruik gemaakt moet worden van de enquête/survey, polls functionaliteit van de leverancier van de betreffende website of de gemeentelijke preferred supplier van enquête/survey/polls functionaliteit (die momenteel nog niet aanwezig is). Dus niet van een buitenstaande derde partij, waar geen overeenkomst mee gesloten kan worden. Het gebruik is afhankelijk van betrouwbaarheidsniveau afhankelijk van betrouwbaarheidsniveau (zie 2.11.1).

Eisen aan enquête/survey functionaliteit:

- Toestemming vragen aan gebruiker en informeren via privacyverklaring
- Verwerkersovereenkomst met (diensten) leverancier
- PKI-overheid certificaat, soort afhankelijk van betrouwbaarheidsniveau, (zie 2.11.1).
- Beveiligde emailvoorziening zie 2.9.1
- De meest recente toegankelijkheidseisen (WCAG)
- Opslag/doorgifte persoonsgegevens op servers binnen de EU (onderdeel van de verwerkersovereenkomst)

2.10 Privacy ontwerprichtlijnen

Privacy by design: houdt in dat je bij het ontwerpen van producten en diensten ervoor zorgt dat je persoonsgegevens goed beschermt, dat je niet méér gegevens verzamelt dan strikt noodzakelijk voor het doel van de verwerking en dat je je gegevens niet langer bewaart dan nodig.

Privacy by default: wil zeggen dat je standaard alleen de persoonsgegevens verwerkt die noodzakelijk zijn om het specifieke doel te bereiken, en dat je de technische en organisatorische maatregelen

neemt om daarvoor te zorgen. Laat een app bijvoorbeeld niet de locatie van gebruikers registreren als dit niet nodig is. Of zorg er voor dat op je website het vakje: 'Ja, ik wil de nieuwsbrief ontvangen' niet vooraf is aangevinkt. Vraag bovendien niet meer gegevens dan je echt nodig hebt als iemand zich op een nieuwsbrief wil abonneren.

2.11 Betrouwbaarheidsniveaus

Overheden wisselen digitaal gegevens uit met bedrijven en burgers. Authenticatiemiddelen zorgen ervoor dat de overheden weten met wie ze van doen hebben. Deze middelen zijn er op verschillende betrouwbaarheidsniveaus. Het niveau hangt af van de aard van de transactie en de gevolgen ervan (zoals financieel of juridisch). Het Forum Standaardisatie heeft een handreiking gemaakt die beleidsmakers, architecten, informatiebeveiligers, juristen en bestuurders helpt om een duidelijke keuze te maken voor het betrouwbaarheidsniveau dat nodig is. [5]

[5] https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus

2.11.1 Indeling betrouwbaarheidsniveau 's

	Betrouwbaarheidsniveau 1	Betrouwbaarheidsniveau 2	Betrouwbaarheidsniveau 3
Kenmerken	Kenmerken: • Hoofddomeinen • Veel interactie • Aard van persoonsgegevens: o Er worden bijzondere persoonsgegevens gebruikt o Betrouwbaarheidsniveau: substantieel o Klasse II Persoonsgegevens (verhoogd) risico • Authenticatiegegevens o DigiD (eIDAS), eHerkenning • Risico's o Groot risico identiteitsfraude o De politiek verantwoordelijke komt in problemen o Er is sprake van klachten, er verschijnen berichten in de media.	Kenmerken: • Subsites / sites derden • Enigszins interactie • Aard van persoonsgegevens: o Er is sprake van een beperkt aantal (niet-bijzondere) persoonsgegevens per individu. o Er is sprake van één type vastlegging, bijvoorbeeld één aanmelding of klantrelatie o Betrouwbaarheidsniveau: laag Klasse I persoonsgegevens (basis) • Authenticatiegegevens o Username / wachtwoord • Risico's o Beperkt risico identiteitsfraude o Er is sprake van klachten, er verschijnen berichten in de media.	Kenmerken: • Subsites / sites derden • Geen interactie of interactie nihil • Aard van persoonsgegevens: o Er worden geen persoonsgegevens verwerkt o Het gaat om openbare persoonsgegevens waarvan algemeen aanvaard is dat deze geen risico opleveren voor de betrokkene o Betrouwbaarheidsniveau: geen Klasse 0 persoonsgegevens • Authenticatiegegevens o Username / wachtwoord • Risico's o Risico identiteitsfraude nihil o Er is sprake van klachten, er verschijnen berichten in de media.
Voorbeelden	Online formulieren t.b.v. digitale dienstverlening, digitaal loket.	Aanmelding nieuwsbrieven, enquêtes, online formulieren.	Combinatie postcode/huisnummer (mijnafvalwijzer.nl).

	Betrouwbaarheidsniveau 1	Betrouwbaarheidsniveau 2	Betrouwbaarheidsniveau 3
Beveiligingscertificaat	**PKI-overheid standaard SSL** Standaard PKI-overheid Looptijd minimaal 1 of 2 jaar, groen slotje *Toepassingen:* • Beveiligen digitale loketten, andere internetdiensten en webshops • Beveiligen server-to-serververkeer, bijvoorbeeld tussen webserver en e-mailservers	**PKI-overheid standaard SSL** Standaard PKI-overheid Looptijd minimaal 1 of 2 jaar, groen slotje *Toepassingen:* • Beveiligen formulieren, enquêtes en ingevulde gegevens • Beveiligen server-to-serververkeer, bijvoorbeeld tussen webserver en e-mailservers	**Xolphin SSL Beveiligingscertificaat** Organisatie validatie
Internetstandaarden	Voldoen	Voldoen	Voldoen
Scannen en pentesten	Maandelijkse scan, jaarlijkse pentest	Halfjaarlijkse scan	Jaarlijkse scan
TPM-verklaring	Jaarlijks verplicht, uiterlijk in oktober aanleveren	Optie	n.v.t
Versiebeheer	Geen oude software, actuele beveiligingspatches	Geen oude software, actuele beveiligingspatches	Geen oude software, actuele beveiligingspatches
Wachtwoordenbeheer	Wachtwoord beheer: minimaal 10 karakters 1 hoofdletter, 1 cijfer, 1 speciaal teken, geen generiek account, halfjaarlijks verversen. Eisen moeten worden afgedwongen door de software.	Beheer: minimaal 10 karakters 1 hoofdletter, 1 cijfer, 1 speciaal teken, geen generiek account, halfjaarlijks verversen. Gebruikers: Minimaal 8 karakters 1 hoofdletter, 1 kleine letter, 1 cijfer, 1 speciaal teken, half jaarlijks verversen. Eisen moeten worden afgedwongen door de software.	Beheer: minimaal 10 karakters 1 hoofdletter, 1 cijfer, 1 speciaal teken, geen generiek account, halfjaarlijks verversen. Eisen moeten worden afgedwongen door de software. Gebruikers: Minimaal 8 karakters 1 hoofdletter, 1 kleine letter, 1 cijfer, 1 speciaal teken.
Authenticatiemethode beheer	Beheer: 2FA	Beheer: 2FA	Beheer: 2FA
Authenticatiemethode gebruikers	Inwoners gebruiken DigiD (e-IDAS) en bedrijven e-Herkenning.	Gebruikersnaam en wachtwoord	Gebruikersnaam en wachtwoord
Contract / SLA	Contract, SLA en verwerkersovereenkomst	Contract, SLA, verwerkersovereenkomst (indien van toepassing)	Contract, SLA, verwerkersovereenkomst (indien van toepassing)

	Betrouwbaarheidsniveau 1	Betrouwbaarheidsniveau 2	Betrouwbaarheidsniveau 3
Applicaties (derden)	• Gebruik maken van formulierenvoorziening leverancier website of preferred supplier • Gebruik maken van nieuwsbrief functionaliteit leverancier website of preferred supplier. • Gebruik maken van enquête/survey, polls functionaliteit leverancier website of preferred supplier.	• Gebruik maken van formulierenvoorziening leverancier website of preferred supplier • Gebruik maken van nieuwsbrief functionaliteit leverancier website of preferred supplier. • Gebruik maken van enquête/survey, polls functionaliteit leverancier website of preferred supplier.	• Gebruik maken van formulierenvoorziening preferred supplier • Gebruik maken van nieuwsbrief functionaliteit preferred supplier. • Gebruik maken van enquête/survey, polls functionaliteit preferred supplier.
Privacy ontwerprichtlijnen	**Privacy by design:** houdt in dat bij het ontwerpen van producten en diensten ervoor gezorgd wordt dat persoonsgegevens goed worden beschermt, dat niet méér gegevens worden verzamelt dan strikt noodzakelijk voor het doel van de verwerking en dat gegevens niet langer bewaard worden dan nodig. **Privacy by default:** wil zeggen dat standaard alleen de persoonsgegevens verwerkt worden die noodzakelijk zijn om het specifieke doel te bereiken, en dat de technische en organisatorische maatregelen genomen worden om daarvoor te zorgen. Vraag bovendien niet meer gegevens dan echt noodzakelijk is.		

3 Toegankelijkheidsbeleid websites

Het is voor overheden al jarenlang verplicht om websites toegankelijk te maken. Dit was vastgelegd in het 'pas toe of leg uit'-beleid. Per 1 juli 2018 is deze verplichting overgegaan in een *wettelijke* verplichting; het Tijdelijk besluit digitale toegankelijkheid overheid. Het idee is dat digitale informatie toegankelijk moet zijn voor iedereen. Naast het faciliteren van mensen met een beperking betekent digitale toegankelijkheid ook dat websites goed werken op bijvoorbeeld een smartphone. Met de komst van de wet is er een tijdlijn opgesteld wanneer websites moeten voldoen aan de digitale toegankelijkheidseisen. Digitaal toegankelijk betekent dat websites moeten voldoen aan de meest recente Web Content Accessibility Guidelines (WCAG). Bij de aanpak hiervan worden gemeenten ondersteund door Logius via de website www.digitoegankelijk.nl.

In april 2020 hebben de H2O-gemeenten een plan opgesteld om de gemeentelijke websites te laten voldoen aan de toegankelijkheidseisen. Dit plan is uitgevoerd. In oktober 2021 is een plan van aanpak opgesteld om ook de pdf-bestanden op de gemeentelijke websites te laten voldoen aan de eisen. Dit plan wordt momenteel uitgevoerd.

3.1 Tijdlijn

Vanaf 23 september 2019:
Alle (interne en externe) websites gepubliceerd vanaf 23 september 2018 moeten digitaal toegankelijk zijn.

Vanaf 23 september 2020:
Alle (interne en externe) websites gepubliceerd vóór 23 september 2018 moeten digitaal toegankelijk zijn.

Uiterlijk 23 juni 2021:
Mobiele applicaties moeten uiterlijk 23 juni 2021 voldoen aan de Wet Digitoegankelijkheid.

3.2 Wat is toegankelijkheid?

Onder toegankelijkheid wordt verstaan dat websites en apps waarneembaar, bedienbaar, begrijpelijk en robuust moeten zijn. Gemeenten moeten ervoor zorgen dat hun websites en/of mobiele applicaties toegankelijk zijn conform de meeste recente versie van de Web Content Accessibility Guidelines. Concreet gaat het hierbij om tekstalternatieven voor bijv. afbeeldingen, ondertiteling, geluid, video, lay-out, kleur, contrast, verwerkingstijd en navigatie. Dat betekent dat bijvoorbeeld documenten ook automatisch moeten worden voorgelezen (door voorleessoftware die niet perse op de website hoeft te worden aangeboden) en dat opnames van raadsvergaderingen die worden getoond via de website moeten zijn voorzien van ondertiteling en audiodescriptie.

De toegankelijkheidseisen hebben betrekking op de volgende componenten op de website:

- Afbeeldingen
- Geluid en video
- Animaties
- Formulieren
- Geo-informatie
- Navigatie
- Tabellen
- Techniek en code
- Tekst

- Vormgeving

Een ‘eenvoudige’ uitleg staat op https://www.digitoegankelijk.nl/uitleg-van-eisen

NB*:* Er zijn momenteel een aantal specifieke situaties en uitzonderingen voor bijvoorbeeld pdf’s, filmpjes, online kaarten, archieven, social media en intranetten. Uitzonderingen zijn onder andere:

- Live uitgezonden, tijdgebonden media (zoals live raadsvergaderingen in audio of video).
- Vooraf opgenomen, op tijd gebaseerde media, die zijn gepubliceerd voor 23 september 2020
- Van derden afkomstige content die niet door de gemeente wordt gefinancierd of ontwikkeld en evenmin onder haar verantwoordelijkheid valt. Als je invloed hebt op de wijze waarop leveranciers inhoud aanleveren, dan ben je verplicht om te zorgen dat de content wel voldoet en dat hiervoor nieuwe afspraken worden gemaakt.
- Pdf-bestanden die voor 23 september 2018 zijn gepubliceerd op een website, tenzij ze onderdeel zijn van een administratief proces dat nog loopt op het moment dat de betreffende website aan de wetgeving moet voldoen. Dat is voor de meeste websites 23 september 2020. (zie ook: https://www.digitoegankelijk.nl/wetgeving/specifieke-situaties/kantoorbestandsformaten);
- Online kaarten en –karteringsdiensten. Maar: kaarten voor navigatiedoeleinden moeten wel op toegankelijke wijze worden verstrekt;
- Reproducties van stukken uit erfgoedcollecties die niet volledig toegankelijk kunnen worden gemaakt om redenen van bewaring, authenticiteit of het ontbreken van geautomatiseerde en kostenefficiënte oplossingen om toegankelijkheid te bewerkstelligen.

Reikwijdte richtlijn: alle overheidsinstanties, zelfstandige bestuursorganen (zbo’s) en gemeenschappelijke regelingen. Private instellingen die uitvoering geven aan een overheidstaak vallen ook onder de werking van het besluit.

Dit betekent dat niet alleen de websites van de gemeenten Hattem, Heerde en Oldebroek onder het besluit vallen, maar ook websites waar de gemeente aan meebetaalt of medeopdrachtgever voor is.

3.3 Toetsing

Toetsing hoofdsites en subsites (technisch en redactioneel) door externe partij (bijv. stichting Accessibility) elke 2 jaar.

De uitvoering en toetsing van digitoegankelijkheid vraagt om een continue proces van verbetering. Omdat digitoegankelijkheid zowel over de technische als de inhoudelijke (content) kant van een website gaat, is nauwe samenwerking tussen functioneel beheer, ICT-adviseurs en beheerders van een website nodig.

Toegankelijkheidsbeleid websites:

- De website voldoet aan de meest recente Web Content Accessibility Guidelines (WCAG).
- Op de website staat een toegankelijkheidsverklaring, aangemaakt met de invulassistent van Logius (zie www.toegankelijkheidsverklaring.nl). Gemeenten zijn verplicht om verantwoording af te leggen over de toegankelijkheid van de digitale kanalen (volgens model Europese Commissie).

4 Archivering van websites en intranetten

Op 20 december 2018 heeft de Standaardisatieraad Nationaal Archief de definitieve versie vastgesteld van de Richtlijn archiveren overheidswebsites. In deze richtlijn worden de regels (de norm) voor de webarchivering in Nederland aangegeven.

4.1 Waarom websites archiveren?

Gemeentelijke websites moeten gearchiveerd worden vanwege de Archiefwet. Dit dient een aantal verschillende belangen:

- Uitvoering bedrijfsprocessen
  Bij het uitvoeren van taken kan het voor overheidsorganisaties nodig zijn om oude webpagina's te bekijken. Bijvoorbeeld voor het beantwoorden van vragen van burgers of het opstellen van rapportages. Ook kan de inhoud van oude websites soms hergebruikt worden. Veel ambtenaren gebruiken websites als naslagwerk bij hun dagelijks werk.

- Verantwoording over overheidshandelen
  Overheidsorganisaties moeten zich kunnen verantwoorden over hun handelen. Websites zijn een belangrijke neerslag van dat handelen. De originele inhoud van de websites moet daarom toegankelijk zijn op het moment dat het handelen ter discussie staat. Dat kan nodig zijn voor het behandelen van WOB verzoeken of in een debat. Maar ook bij een parlementair- of raadsonderzoek, een audit of rekenkameronderzoek.

- Recht- en bewijszoekende burgers
  Burgers en bedrijven kunnen rechten ontlenen aan informatie op websites. Bijvoorbeeld bij het aanvragen van diensten, vergunningen, subsidies, of het starten van een bedrijf. Burgers en bedrijven baseren keuzes en handelingen op de informatie van de overheid. Die informatie kan daarom nodig zijn als bewijs in beroeps- en bezwaarprocedures. Als een overheidsorganisatie een zaak verliest omdat ze niet beschikt over dit bewijsmateriaal, dan kan dat leiden tot hoge kosten en imago- of gezichtsverlies.

- Recht- en bewijszoekende medewerkers / verantwoording interne werkprocessen
  Medewerkers kunnen rechten ontlenen aan informatie op het Intranet. Bijvoorbeeld wanneer hier regelingen of werkafspraken zijn geplaatst. Medewerkers kunnen hun keuze bepalen aan informatie dat op een specifiek moment is geplaatst op het intranet. Deze informatie kan nodig zijn in beroeps- en bezwaarprocedures. De organisatie zelf moet beschikken over een weergave van de informatie die is geplaatst.

- Onderzoek
  Overheidswebsites geven onderzoekers inzicht in hoe overheidsorganisaties hun taken uitvoerden en zichzelf presenteerden. Bijvoorbeeld als er onderzoek gedaan wordt naar de aanpak van een grote crisis, naar hoe bepaalde besluiten tot stand zijn gekomen, of naar de relatie tussen overheid en burgers.

- Erfgoed
  Websites zijn ook een uiting van onze cultuur. Niet alleen de inhoud, maar bijvoorbeeld ook de vormgeving en het taalgebruik. Op het moment dat een website nog volop gebruikt wordt is het misschien moeilijk voor te stellen. Maar ooit zullen websites hetzelfde gevoel opwekken als het Polygoonjournaal en verkleurde jaren 70-foto's. Die willen we nu niet meer missen omdat ze ons herinneren aan het verleden en medebepalen hoe we ons zelf zien.

4.2 Welke websites moet de gemeente archiveren en voor hoe lang?

Dat hangt af van wat voor soort website het is, de belangen die ermee gemoeid zijn en de kosten (bron: Richtlijn archiveren overheidswebsites voor Publiekscommunicatie, mei 2018). Het maken van deze afwegingen is onderdeel van het archiveringsproces. In algemene zin geldt alle openbare websites van (semi)overheidsinstanties moeten worden gearchiveerd volgens de Archiefwet.

4.2.1 Welke websites moet je archiveren?

Met openbare websites wordt bedoeld: het hoofddomein, subdomeinen en overige domeinen die vallen onder verantwoordelijkheid van de gemeente. Websites moeten blijvend bewaard worden volgens de Archiefwet en na 10 jaar in een archiefbewaarplaats terecht komen, alwaar ze kosteloos te raadplegen zijn. Ook als de informatie niet beeldbepalend is voor de burger, geldt nog een bewaartermijn van 10 jaar.

4.2.2 Hoelang bewaren in een archiefbewaarplaats?

Met het archiveren van websites wordt het bewaren van de informatie op webpagina's bedoeld. Voor het bepalen hoelang deze informatie bewaard moet worden, wordt de selectielijst van de VNG gevolgd. Dit geldt voor webpagina's van websites waar de overheidsorganisatie zelf het beheer uitvoert en voor webpagina's van websites waar de overheidsorganisatie mede-beheerder is.
De contenteigenaar is verantwoordelijk voor archivering van de eigen content op een gedeelde website. Het gedeeltelijk bewaren van pagina's is in de praktijk lastig, waardoor meestal een beheerder wordt aangewezen die verantwoordelijk is het archiveren van de website.

Op termijn vernietigbare webpagina's bevatten eigenlijk alleen die informatie die volgens de selectielijst ook vernietigd mag worden. In de praktijk is dit niet goed uitvoerbaar, omdat webpagina's naar elkaar verwijzen en onderdeel zijn van een volledige website. Dan is het beter om deze pagina's ook permanent te bewaren.

Als een website (of eigenlijk de webpagina's) gearchiveerd moet worden, moet dit dus permanent gebeuren.

4.3 Eisen

In de 'Richtlijn archiveren overheidswebsites' worden alle eisen benoemd. De hoofdlijnen van de eisen betreffen de volgende eisen:

- alle openbare websites van (semi)overheidsinstanties moeten worden gearchiveerd volgens de Archiefwet. Met de openbare websites wordt bedoeld: het hoofddomein, subdomeinen en overige domeinen die vallen onder verantwoordelijkheid van de gemeente;
- de frequentie van archiveren is 'dagelijks'. Bij veel veranderingen op dezelfde dag, zou een handmatige overdracht/opslag beter zijn.
- de archieven moeten permanent en duurzaam worden bewaard.

Voor een volledig overzicht van de eisen zie de Richtlijn archiveren overheidswebsites.

4.4 e-Depot

Streekarchief Epe Heerde Hattem is in 2019 gestart met de voorbereidingen voor het ontwikkelen van of aansluiten bij een e-Depot. Met het e-Depot wordt ingezet op het duurzaam bewaren van digitale informatie. Ook is het Streekarchief Epe Heerde Hattem in overleg met het Streekarchivariaat Noordwest-Veluwe (SNWV) voor verdergaande samenwerking.

Voor het Streekarchief is een businesscase is opgesteld voor het zelf ontwikkelen van of het aansluiten op een bestaand e-Depot. In H2O-verband is een visie ontwikkeld op het gebied van duurzaam

informatiebeheer en in samenhang daarmee het aansluiten op een e-Depot. De visie is ontwikkeld in samenwerking met Epe. De visie richt zich in principe op het aansluiten bij een bestaand e-depot.

Oldebroek is aangesloten bij het SNWV. SNWV heeft een eigen e-Depot. SNWV heeft het inkooptraject uitgevoerd in samenwerking met de aangesloten gemeenten. Er is een inkooptraject uitgevoerd en een leverancier (Picturae) voor de software en hosting gekozen.

Of er een koppeling tussen de huidige archiveerder van de websites (Archiefweb) en het e-Depot wordt gerealiseerd, moet nog worden bepaald en uitgewerkt. Dat geldt ook voor de wijze waarop een dergelijke koppeling vormgegeven moet worden.

4.5 Tenslotte

Elke overheidsorganisatie is verantwoordelijk voor de archivering van zijn eigen websites. Het toepassen van deze norm is daarbij vrijwillig maar niet vrijblijvend. Als een overheidsorganisatie deze norm niet toepast, dan zal ze op een andere manier moeten voldoen aan de verplichting van de Archiefwet 1995 om haar websites te archiveren.

Archiveringsbeleid websites:

- Alle openbare websites van (semi)overheidsinstanties moeten worden gearchiveerd volgens de Archiefwet.
- De frequentie van archiveren is ‘dagelijks’. Bij veel veranderingen op dezelfde dag, zou een handmatige overdracht/opslag beter zijn of in mogelijk moeten zijn.
- De archieven moeten permanent en duurzaam worden bewaard.

5 Beheer websites

5.1 Beheer websites Hattem, Heerde en Oldebroek

Team Communicatie is het aanspreekpunt voor alle communicatie-uitingen. Het beheer van de gemeentelijke hoofdwebsites, subsites (die in hetzelfde CMS als de hoofdwebsites staan) en de participatieplatformen van Citizenlab vallen binnen de scope van team Communicatie (Hattem en Oldebroek) of afdeling Dienstverlening en Informatiebeheer (Heerde). Een overzicht van deze websites staan in de bijlage (Excel bestand).

Team Communicatie/afdeling Dienstverlening en Informatiebeheer is verantwoordelijk voor het functioneel beheer van de hoofdwebsites en subsites. Het functioneel beheer van het participatieplatform ligt bij de leverancier.

Het beheer van alle overige websites van de H2O-gemeenten is belegd bij de betreffende vakafdeling of bij een externe partij. De vakafdelingen zijn verantwoordelijk voor de juistheid en actualiteit van de content van alle websites. Team communicatie/ afdeling Dienstverlening en Informatiebeheer kan ondersteuning bieden voor toegankelijke webteksten en formulieren.

5.2 Huisstijl websites en portalen

Het bewaken van de huisstijl is belegd bij team Communicatie. Op dit vlak moet er altijd een check/betrokkenheid van een communicatieadviseur zijn voor een website/portaal live gaat. Of de huisstijl wordt toegepast (dit kan een keuze zijn) en welke huisstijl wordt bepaald in overleg met team Communicatie. Dit is dan ook geen onderdeel van het technisch websitebeleid.

5.3 Aanvraag nieuwe website

Voor het aanvragen van een nieuwe website gelden tenminste de volgende processtappen. Dit is inclusief de toets door communicatie op passendheid in de communicatiemix en toepassing van huisstijl.

Stap 1 - Doel en uitgangspunten bepalen:

- Doel website (check door communicatie: past dit in het grotere geheel en de communicatiemix)
- Bepalen of de nieuwe website in het CMS van de voorkeursleverancier kan worden opgenomen; indien geen gebruik gemaakt wordt van de voorkeursleverancier waar gaat de website dan draaien?
- Uren/budget benodigd voor functioneel en technisch beheer, toegankelijkheid en archivering
- Looptijd van de website en datum livegang
- Benodigde functionaliteiten (bijv. e-formulieren, nieuwsbrieven, enquêtes, internetkassa, authenticatiemiddelen)
- Betrouwbaarheidsniveau bepalen (aard van de persoonsgegevens, certificaat, pentest ja of nee)

Let op: Indien de website niet ontwikkeld kan worden op een reeds aanwezig CMS, moet er een verzoek ingediend worden bij het Wijzigingsadviescommissie (WAC). Met het verzoek kan dan een onderzoek worden ingesteld of de gewenste functionaliteiten en keuze van een (andere) leverancier gerechtvaardigd zijn en voldoen aan de gestelde criteria.

Huidige websiteleverancier H2O: Roxit/GreenValley

Stap 2 - Offerte en ontwikkelfase:

- Offerte(s) aanvragen voor Content Management Systeem (CMS) en indien nodig hosting
- Afstemming met leverancier over onder andere de planning

- Beveiligingscertificaat (laten) aanvragen
- Offertes aanvragen voor in ieder geval archivering van de website en toegankelijkheidsinspectie. En eventueel voor andere benodigde functionaliteiten.
- Ontwikkelen website
- Aanleveren content (inhoud) website
- Testen van de website

Stap 3 - Acties voor livegang:
De website

- wordt gecheckt of deze voldoet aan:
    - Beveiliging- en privacybeleid
    - Toegankelijkheidsbeleid
    - Archivering
    - Beheer
    - Huisstijl beleid
- is voorzien van:
    - een toegankelijkheidsverklaring
    - indien vereist een privacyverklaring of een verwijzing naar de privacyverklaring op de hoofdwebsite
    - indien vereist een cookieverklaring
    - indien gewenst een Google Analytics code t.b.v. statistieken
- beschikt over:
    - een contract
    - een SLA (Service Level Agreement)
    - indien nodig een verwerkersovereenkomst

5.4 Onderhoud en beheer

Voor het onderhouden en beheren van de websites van de gemeente wordt een overzicht van websites opgesteld en jaarlijks geactualiseerd. In het overzicht van websites zijn de volgende activiteiten benoemd voor het toetsen en optimaliseren van de websites:

- Contract, SLA, verwerkersovereenkomst aanwezig en actueel
- Scoort 100% op de eisen van internet.nl en A+ bij SSLLab.com
- Wordt gearchiveerd
- Bevat een actuele toegankelijkheidsverklaring
- Bevat (indien vereist) een actuele privacyverklaring
- Bevat (indien vereist) een actuele cookieverklaring
- Voldoet aan huisstijl
- Bevat actuele en betrouwbare content
- Pentesten
- Is voorzien van de meest recente versie van het CMS

Beheer websites:

- Voor het aanvragen van een website volgen we een vaste procedure.
- Websites worden onderhouden en het beheer gebeurt m.b.v. een beheerplan (zie bijlage Format beheerplan).
- Huisstijl wordt altijd afgestemd met team communicatie.
- Websites beheerd door derden of (dienstverlenings-)portalen moeten ook voldoen aan de eisen die gelden voor overheidswebsites.
- Jaarlijks wordt verantwoording afgelegd over het onderhoud en beheer.