Bijlage 2 - Eisen t.a.v. oplossing en dienstverlening

1.1 Functioneel

#	Omschrijving	Eis / Wens
1	U-veilig.nl is één digitale plek voor burgers, bedrijven en pers in de regio Utrecht waar zij eenduidige en actuele informatie kunnen vinden over risico's, incidenten, rampen en crises in hun regio. U-veilig is een digitaal platform met risicocommunicatie (statisch en dynamisch) en crisiscommunicatie voor burgers, bedrijven en pers. In de koude situatie is informatie over het risicoprofiel en (B)VL te vinden. In de lauwe fase is informatie te vinden over waarschuwing ten aanzien van bijvoorbeeld extreem weer en bijbehorende handelingsperspectieven. Met het middel U-veilig verbinden we in de warme fase de crisiscommunicatie door woordvoerders (zoals die nu via twitter wordt gedaan) met relevante handelingsperspectieven. Er kan worden doorgeklikt naar verdere informatie die staat op brandweer.nl, vru.nl en u-veilig zelf, de bezoeker ziet deze informatie binnen de 'look and feel van U-veilig. Op één plek ziet de bezoeker de informatie van de woordvoerder, een kaart met de incidentlocatie en relevante handelingsperspectieven. Woordvoerders kunnen eenvoudig informatie plaatsen via een app op hun device en met één druk op de knop de informatie delen via Twitter (en eventuele andere kanalen) waarbij de lezer naar U-veilig wordt doorverwezen voor alle relevante informatie. Het platform is onderdeel van vru.nl. de corporate website die op dit moment wordt vernieuwd. In de toekomst is er één externe website voor al onze doelgroepen (alle bezoekers komen binnen op vru.nl en de look and feel is gelijk voor alle onderdelen). De oplossing dienst op basis van een proven concept te zijn.	Eis
2	Aan alle content moet een termijn (bijvoorbeeld 5 jaar) worden toegekend en volgt een melding bij het verlopen van de termijn (aan de persoon die plaatst en beheerder van de site).	Wens
3	Via sitestatistieken kunnen gemakkelijk cijfers en rapportages ontsloten worden.	Eis
4	De website heeft een voorleesfunctie, deze moet digi-toegankelijk worden toegepast conform EN301549 met WCAG2.1 niveau A en AA standaard.	Eis
5	Het systeem heeft een goede zoekfunctie, zowel aan voor- als achterkant.	Eis
6	Er moet sprake zijn van een Koppeling met de website vru.nl: • Bezoekers komen op vru.nl binnen (extern wordt één site in de markt gezet), voor de homepage en pagina's die verband houden met wat is beschreven onder U-veilig geldt: De website is berekend op hoge aantallen bezoekers (zie geformuleerde eis), dit kan gezien het doel (bijvoorbeeld na een NL-Alert) exponentieel toenemen. De geleverde hostingcapaciteit dient schaalbaar te zijn, dit kan automatisch aan de hand van het sitegebruik. Tijdens dagelijks gebruik zal het bezoekersaantal veel lager liggen. Tijdens een calamiteit zal de geschatte belasting het volgende zijn: 4000 pageviews per seconde. 20 redacteuren, 10 eindredacteur rollen. • Nieuw vru.nl wordt met drupal gebouwd op dit moment.	Eis

#	Omschrijving	Eis / Wens
7	De website laat zich snel bijwerken, content updates worden direct doorgevoerd. De nieuwe website biedt de gebruikers dat wat conform een moderne en snelle website verwacht mag worden. Hierbij gelden minimaal de volgende zaken: • Oproepen van een pagina in het CMS duurt maximaal 1,5 seconden (gemeten nadat de opdracht is gegeven en er voor de gebruiker zichtbaar resultaat is op zijn/haar scherm) • De mutatie van een pagina in het CMS dient binnen 2 seconden opgeslagen te zijn, zodat het vervolgscherm weer getoond wordt • Na het ingeven van een zoekopdracht zijn de zoekresultaten binnen 2 seconden voor een gebruiker zichtbaar. • Opgevraagde pagina's dienen binnen 1 seconde beschikbaar te zijn. • Uploaden van een bestand van 2 MB naar het CMS duurt maximaal seconden. • Downloaden van een bestand 2 MB duurt maximaal 4 seconden • Rapportages dienen binnen 10 seconden uitgevoerd te worden waarna de resultaten zichtbaar zijn voor de gebruiker op het scherm. • Een nieuwsbrief (of weekoverzicht) dat gestuurd wordt naar alle abonnees wordt binnen 1 uur verstuurd. • Batchprocessen hebben geen negatief effect op de performance van de website, zowel voor bezoekers van de website(s) als voor gebruikers. • Gelijktijdig met meerdere gebruikers in het CMS bewerkingen uitvoeren leidt niet tot terugloop in reactietijd ofwel: 10 redacteuren kunnen tegelijkertijd in het CMS aan het werk zijn zonder enige nadelige invloed op de performance. • Er is sprake van versiebeheer, er moet zichtbaar zijn wie de redacteur is wanneer de laatste wijziging is gedaan (in het CMS).	Eis
8	Er moet sprake zijn van een Koppeling met de website vru.nl: • Bezoekers komen op vru.nl binnen (extern wordt één site in de markt gezet), voor de homepage en pagina's die verband houden met wat is beschreven onder U-veilig geldt: De website is berekend op hoge aantallen bezoekers (zie geformuleerde eis), dit kan gezien het doel (bijvoorbeeld na een NL-Alert) exponentieel toenemen. De geleverde hostingcapaciteit dient schaalbaar te zijn, dit kan automatisch aan de hand van het sitegebruik. Tijdens dagelijks gebruik zal het bezoekersaantal veel lager liggen. Tijdens een calamiteit zal de geschatte belasting het volgende zijn: 4000 pageviews per seconde. 20 redacteuren, 10 eindredacteur rollen. • Nieuw vru.nl wordt met drupal gebouwd op dit moment.	Eis
9	De app voor woordvoerders moet te gebruiken zijn voor mensen met een device van de VRU en door mensen zonder device van de VRU.	Eis
10	De woordvoerders kunnen via een gebruiksvriendelijke app op hun telefoon, tablet en laptop woordvoering doen welke gepubliceerd kan worden op de site, twitter en andere (sociale media) kanalen. In lijn met de eisen die aan een app gesteld worden.	Eis
11	Bij incidenten wordt de bezoeker een toegankelijke manier vanaf vru.nl naar de incidentomgeving van U-veilig geleid. Een bezoeker kan ook via een directe URL of via een link in de berichtgeving van een Operationeel Woordvoerder op social media. Op deze plek vindt de bezoeker een interactieve kaart waarop door middel van een basiskaart, (incident)locaties kunnen worden vastgelegd. Op deze plek ziet de bezoeker ook de informatie die wordt ingevoerd door de woordvoerder en handelingsperspectief dat hoort bij het type incident (op basis van een vooraf gevulde database met handelingsperspectieven.	Eis

#	Omschrijving	Eis / Wens
12	Het moet mogelijk zijn een tweede interactieve kaart van de provincie te maken waarop risico's kunnen worden aangegeven. Voor een aantal onderwerpen kan het actuele risico worden aangegeven met een kleurcodering. Hierin kan samengewerkt worden met derden (denk aan het KNMI bij kleurcodes over het weer).	Wens
13	Afgeschermd moeten pagina's met informatie en doorlinks kunnen worden geplaatst, die toegankelijk zijn voor mensen met een inlogcode.	Wens

Hieronder worden de niet-functionele eisen beschreven m.b.t. de oplossing en de eisen m.b.t. de dienstverlening door Leverancier.

1.2 Algemeen

#	Omschrijving	Eis / Wens
14	U-Veilig is niet alleen beschikbaar als website, maar ook te downloaden als app via Androïd, Apple en Google.	Eis
15	Gebruikers van U-veilig.nl kunnen desgewenst een berichtje op hun mobiel krijgen tijdens een incident. Zij kunnen deze berichtgeving desgewenst finetunen d.m.v. locatiegegevens (net zoals bij een NL Alert). Daarnaast kunnen zij desgewenst ook gealarmeerd worden indien er een incident is op andere locaties dan waar zij zich bevinden. (bijvoorbeeld: school kinderen, woonadres ouders, thuisadres, werkadres, etc)	Eis
16	Leverancier conformeert zich aan de eisen van de GIBIT 2020 en ICT-kwaliteitsnormen voor de Veiligheidsregio1.	Eis
17	Leverancier voldoet aan alle eisen zoals gesteld in de AVG2	Eis
18	(Zoals in GIBIT-artikel 8.6) Voor de beheer- en onderhoudsfase na de implementatie, zal een SLA worden opgesteld tussen de VRU en Leverancier, waarin de afgesproken dienstverlening wordt vastgelegd op het gebied van o.a.: • Incidenten en Changes en werkwijze daaromtrent; • Reactietijden, oplostijden, onderhoudstijden; • Beheer, Onderhoud en werkwijze; • Nederlandstalige Helpdesk en gebruikersondersteuning; • Rapportage en overleggen op diverse niveaus; • Evaluaties.	Eis
19	Leverancier rapporteert aan de VRU over de in de SLA overeengekomen servicelevels en KPI's. Periodiek wordt gerapporteerd over de afgesproken indicatoren met aggregatieniveau van 1 kalendermaand, bijv. • Aantal calls, openstaand en afgehandeld; • Hoeveelheid gemelde incidenten, classificatie en oplostijden verdeeld naar categorie; • Aantal escalaties, inclusief evaluatie.	Eis
20	Voor het bewaken van de afgesproken kwaliteit, het realiseren van de afgesproken servicelevels en het doorvoeren van veranderingen en verbeteringen (vastgelegd in evt. verbeterplannen) is regelmatig overleg op diverse organisatieniveaus noodzakelijk. Periodiek vindt overleg plaats tussen de VRU en Leverancier over deze KPI's / performance. Daarnaast zullen in het kader van verlengingen van het contract evaluaties tussen beide Partijen plaatsvinden. Deze structuren worden vastgelegd in de SLA.	Eis

1 De Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) zijn te vinden in Bijlage D1 – GIBIT 2016 en de ICT-Kwaliteitsnormen voor Veiligheidsregio's zijn te vinden in Bijlage D2 – ICT-Kwaliteitsnormen 2020 bij GIBIT
2 De wet AVG zoals beschreven op: https://wetten.overheid.nl/jci1.3:c:BWBR0040940&z=2020-01-01&g=2020-01-01

#	Omschrijving	Eis / Wens
21	Alle gegevens binnen de oplossing, dan wel ter beschikking gesteld aan de leverancier blijven te allen tijde eigendom van de VRU.	Eis
22	Indien de overeenkomst ter rechtswege wordt beëindigd dienen alle gegevens van de VRU ter beschikking worden gesteld.	Eis
23	De oplossing dient zich in een webbased omgeving te presenteren, die volledig functioneel en remote wordt ondersteund op standaardbrowsers, waarbij minimaal alle recente browsers (waaronder minstens Internet Edge, Chrome, Firefox)worden ondersteund. Hierbij geldt dat minimaal de browser versies van de afgelopen twee jaar dienen te worden ondersteund, bij voorkeur zonder gebruik van extra configuratie, plugins en software, anders dan de standaardconfiguratie. Hierbij is sprake van portabiliteit naar smartphones en tablets.	Eis
24	Het moet mogelijk kunnen zijn op termijn koppelingen of verbindingen aan te gaan met andere systemen (zoals gemeentelijke websites of KNMI).	Eis
25	Het CMS wordt als cloudoplossing aangeboden en is benaderbaar via moderne webbrowsers (o.a. Internet Explorer, Edge, Chrome, Firefox, Safari) zonder dat daarvoor aanvullende software hoeft te worden geïnstalleerd. Het CMS wordt als dienst afgenomen; geen omgeving op servers en/of in beheer van de VRU zelf. De VRU verwacht dat de partij het CMS voor de VRU beheert, waaronder: • Applicatie- en technisch beheer (functioneel beheer, link tussen leverancier en gebruiker, wordt uitgevoerd door de VRU). • Het aantoonbaar beheren en monitoren van de genomen beveiligingsmaatregelen .	
26	Het platform biedt een intuïtieve, marktconforme gebruikersinterface in tenminste de Nederlandse taal.	Eis

1.3 Beschikbaarheid

#	Omschrijving	Eis / Wens
27	Er kan in beginsel 24 uur per dag / 7 dagen per week gebruik worden gemaakt van de oplossing. De beschikbaarheid van de oplossing is voor minimaal 99,9 % 24/7 gegarandeerd. Downtime vanwege installatie- en herstelverzoeken van de VRU wordt niet meegerekend in het meten van deze beschikbaarheid. Gepland beheer en onderhoud, met risico tot downtime, wordt buiten deze tijden uitgevoerd. Gepland onderhoud kan worden uitgesteld in geval van een lopende crisis.	Eis
28	Opdrachtnemer garandeert een toegankelijkheid van de Oplossing van 24 uur / 7 dagen per week, gemeten per kalendermaand, buiten geplande onderhoudstijden, voor die onderdelen van het systeem die op de infrastructuur van de Opdrachtnemer draaien. Deze afspraak wordt nog verder gespecificeerd in de SLA.	Eis

1.4 Projectplan en implementatie

#	Omschrijving	Eis / Wens
29	De leverancier dient voor de uitvoering van het project een projectplan en implementatieplan en indien nodig een migratieplan op te stellen. De basis wordt hiervoor al gelegd in de gunningscriteria.	Eis
30	Indien het voor de oplossing noodzakelijk is dat er installaties plaatsvinden binnen de omgeving van de VRU, dan zijn tijdens installatie van de oplossing (ook in de testfase) de handleidingen voor systeembeheer (inclusief installatieverslag) beschikbaar en worden gespecificeerd voor de inrichting van de VRU.	Eis

#	Omschrijving	Eis / Wens
31	De Leverancier levert de oplossing met een volledig technisch ontwerp/beschrijving van de inrichting bij de VRU. Dit technisch ontwerp beschrijft de wijze waarop de oplossing binnen de ICT- architectuur van de VRU is geïmplementeerd en ingebed. Hierin worden ook de afwijkingen op de architectuur beschreven. *Toelichting: Het betreft niet het technisch ontwerp van de oplossing zelf.*	Eis

1.5 Testen en acceptatie

#	Omschrijving	Eis / Wens
32	De leverancier levert tijdens de implementatiefase een uitgewerkte testaanpak/testplan op. Deze testaanpak wordt afgestemd met de VRU en omvat zowel gebruikerstesten, integratietesten als testen ten aanzien van de uit te voeren datamigratie. Basis voor deze testen zijn de in deze aanbesteding gestelde eisen.	Eis
33	De leverancier levert de oplossing compleet, getest en bedrijfsvaardig op. Dit betekent dat de leverancier de testen moet uitvoeren en de VRU moet voorzien van testverslagen.	Eis
34	De VRU zal een Functionele Acceptatietest uitvoeren. De Functionele Acceptatietest kan betrekking hebben op de oplossing alsmede op iedere afzonderlijke component van de oplossing (de Apparatuur, de Programmatuur, de Inrichting, de Diensten en/of de bijbehorende Documentatie). De Leverancier zal assisteren bij de uitvoering van Functionele Acceptatietest.	Eis
35	De leverancier levert voor go-live een lijst met “known errors” van de oplossing op en een inschatting wanneer deze worden opgelost.	Eis

1.6 Continuïteit en conformiteit

#	Omschrijving	Eis / Wens
36	De leverancier verplicht zich om in het geval van een calamiteit of ramp de afgesproken dienstverlening binnen een half uur te continueren.	Eis
37	De leverancier garandeert d.m.v. backup & restore-procedures dat gegevensverlies maximaal 24 uur kan bedragen.	Eis
38	De leverancier verplicht zich de data redundant op te slaan in geografisch gescheiden fysieke locaties. Deze locaties bevinden zich niet binnen dezelfde dijkring.	Eis
39	De leverancier houdt de aangeboden oplossing proactief in lijn met de landelijke afgesproken standaarden die betrekking hebben op ICT-standaarden.	Eis
40	De aangeboden oplossing volgt de ontwikkelingen binnen moderne browser technologie, zoals nu HTML5 en CSS3 evenals de toekomstige mogelijkheden en ontwikkelingen.	Eis
41	De leverancier heeft met een derde partij een escrow-regeling waaruit blijkt dat continuïteit van het gebruik van de oplossing gewaarborgd is in geval van rampen en calamiteiten (zoals faillissement).	Eis
42	De oplossing beschikt over een rapportage waaruit de integriteit van het systeem blijkt.	Eis
43	De oplossing is toegankelijk en onafhankelijk van tijd en plaats (via bedrijfsnetwerk en direct-access) te gebruiken.	Eis
44	Leverancier draagt zorg dat de aangeboden oplossing compatibel is met de IT Architectuur van de VRU.	Eis
45	Bij het officieel vernietigen van informatieobjecten op basis van de Archiefwet worden ook de objecten uit de back-up vernietigd. Geef aan op welke manier de oplossing hierin voorziet en/of welke procedures hiervoor gelden om te voorkomen dat vernietigde informatieobjecten beschikbaar komen na het terugzetten van een back-up.	Wens

#	Omschrijving	Eis / Wens
46	Archieffunctie – elke versie van de website moet met daytime stamp bewaard worden.	Eis
47	Het is mogelijk individuele informatieobjecten vanuit de back-up te herstellen zonder dat de gehele inhoud van de oplossing teruggezet dient te worden. Dit dient mogelijk te zijn met een retentie van 365 dagen.	Wens

1.7 Informatiebeveiliging

#	Omschrijving	Eis / Wens
48	De leverancier maakt bij de opslag van persoonsgegevens gebruik van fysieke opslag en verwerking binnen de Europese Unie (EER) en zorgt ervoor dat doorgifte van gegevens naar landen buiten de Europese unie uitgesloten is.	Eis
49	Leverancier zorgt voor adequate functiescheiding en daarmee in overeenstemming zijnde Identity & Acces Management zodat slechts bevoegd personeel toegang heeft tot de data. Daarbij zijn verschillende permissie/rechten-niveaus door de Opdrachtgever te configureren na oplevering.	Eis
50	Leverancier is verantwoordelijk voor het gebruik, de behandeling, de bescherming en uitwisseling van vertrouwelijke gegevens die gedeeld worden met zijn onderaannemers. Daarbij is een door Opdrachtgever goedgekeurde verwerkingsovereenkomst van kracht voor leverancier en onderaannemers.	Eis
51	Leverancier zorgt voor minimaal 256 bits versleuteling volgens Advanced Encryption Standard (AES) voor opslag en transport van gevoelige gegevens.	Eis
52	De leverancier treft maatregelen om de kans op hackeraanvallen en/of kwaadaardige software te minimaliseren, waaronder minimaal het in gebruik hebben en up-to-date houden van technologieën als firewalling, antivirus, IDS, IPS en encryptie.	Eis
53	Leverancier zorgt voor patchmanagementbeleid, waarin onder andere informatie staat met betrekking tot hardening van processen (bijvoorbeeld uitschakelen van ongebruikte services, etc.), zodat alle ICT-componenten zijn gehard tegen aanvallen.	Eis
54	De leverancier zorgt voor (fysieke en logische) toegangsbeveiliging en brandpreventie van de IT-systemen.	Eis
55	De oplossing heeft en houdt tijdens de loop van het contract een 100% score op internet.nl	Eis
56	Leverancier maakt gebruik van HTTPS en HSTS voor webverkeer. Zie https://www.forumstandaardisatie.nl/open-standaarden/https-en-hsts. De leverancier maakt hierbij gebruik van een door Opdrachtgever voorgeschreven SSL-certificaat.	Eis
57	Leverancier heeft meldplicht bij de VRU na een security breach / datalek, binnen 24 uur. Opdrachtnemer overlegt eerst met Opdrachtgever in het geval Opdrachtnemer een datalek, welke betrekking heeft op de VRU omgeving, constateert voordat Opdrachtnemer een melding maakt bij de Autoriteit Persoonsgegevens (AP).	Eis
58	Alle door leverancier aangeboden diensten vallen binnen een door leverancier of zijn onderaannemers gebruikt ISMS (Information Security Management System), dat gecertificeerd is conform de ISO27001.	Eis
59	De SoA (Statement of Applicability) van leverancier behorend bij de ISO27001 wordt voor VRU inzichtelijk gemaakt (evt. meegestuurd), of leverancier geeft inzicht in de relevante beheersmaatregelen die zijn ingesteld binnen zijn organisatie.	Eis
60	De leverancier voert periodiek (minimaal 1x per jaar) een pentest en kwetsbaarhedenscan uit op de aangeboden omgevingen. Leverancier verschaft over de uitvoering en de resultaten een jaarlijkse rapportage aan de VRU.	Eis
61	Eventuele gebleken tekortkomingen m.b.t. beveiliging n.a.v. dergelijke beveiligingstest/-audits dienen te worden meegenomen bij de doorontwikkeling van de oplossing (als onderdeel van het onderhoud) en zo nodig op de kortst mogelijke termijn te worden gepatcht.	Eis

#	Omschrijving	Eis / Wens
62	Beveiligingspatches voor het CMS worden zo snel als technisch mogelijk geïnstalleerd	Eis
63	In de rapportage over de dienstverlening is informatiebeveiliging een specifiek onderdeel. Bij het opstellen van de SLA wordt bepaald over welke KPI's er gerapporteerd wordt.	Eis
64	Indien leverancier software ontwikkelt (zelf of via subcontractsoors), hanteert leverancier aantoonbaar het principe "security by design" en “privacy by design”.	Eis
65	De webapplicaties die leverancier aanbiedt, zijn ingericht conform de richtlijnen van het NSCS (Nationaal Cyber Security Centrum) "ICT-Beveiligingsrichtlijnen voor Webapplicaties - Verdieping".	Eis
66	Leverancier heeft met alle onderaannemers een contract met hierin een clausule informatiebeveiliging/geheimhouding.	Eis
67	Medewerkers (en onderaannemers) van leverancier hebben een VOG (Verklaring Omtrent Gedrag) of leverancier heeft een VOG Rechtspersoon.	Eis
68	Leverancier heeft een actieve incidentprocedure m.b.t. de communicatie rondom informatiebeveiligingsincidenten met haar klanten. De VRU wordt door de leverancier benaderd als zij een incident constateren.	Eis
69	De VRU sluit met leverancier een verwerkersovereenkomst af die ook van toepassing is op eventuele onderaannemers van leverancier indien dit nodig mocht zijn als verwerker van persoonsgegevens.	Eis
70	De VRU heeft te allen tijde recht op het uitvoeren van een onafhankelijke externe audit of leverancier laat door een onafhankelijke externe partij een audit uitvoeren (minimaal 1x per jaar) en deelt de uitkomst transparant met de VRU.	Eis
71	In het rapport of de bijlage bij de uitkomst van de audit staat wat er is geconstateerd, welke maatregelen leverancier gaat nemen en binnen welke periode dit zal zijn uitgevoerd.	Eis
72	Leverancier heeft een actieve procedure "meldplicht datalekken". Leverancier informeert de VRU hier onmiddellijk na constateren over en geeft aan welke eisen leverancier aan de VRU hierover stelt. Wanneer er sprake is van een datalek vanuit de oplossing door een lek in de software/programmatuur dan dient de leverancier hier direct actie op te ondernemen en de VRU hierop te attenderen. Indien de oorsprong van de oorzaak betrekking heeft op de infrastructuur van VRU dan zal de leverancier de VRU daarop direct moeten attenderen alsmede te adviseren wat de VRU daaraan kan doen.	Eis
73	Leverancier overlegt eerst met de VRU in het geval leverancier een datalek constateert voordat leverancier een melding maakt bij de Autoriteit Persoonsgegevens (AP).	Eis
74	Leverancier is in staat voor de afgenomen dienst voldoende logging beschikbaar te stellen voor het aanleveren van een audittrail in geval een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens (AP).	Eis
75	In het geval van aanval/security breach dient leverancier verzamelde data ter beschikking te stellen. De data dienen minimaal 60 dagen na aanval nog beschikbaar te zijn. Leverancier stelt de verzamelde data beschikbaar voor eventueel onderzoek bij een derde partij.	Eis
76	De VRU heeft toestemming de componenten/diensten die onderdeel zijn van dienstverlening van leverancier aan de VRU permanent op te nemen in kwetsbaarheden-scanners van VRU.	Eis
77	DDOS bescherming is geactiveerd	Eis
78	Op het moment dat de pagina van u-veilig.nl wordt geopend, krijgen de sociale media bedrijven geen informatie over de bezoeker aan onze site. Op het moment dat de bezoeker doorklikt naar de VRU-pagina op één van de sociale media platforms krijgen die bedrijven pas informatie over de bezoeker van hun site. Ook andere statistieken die bijgehouden worden moeten geanonimiseerd worden.	Eis

#	Omschrijving	Eis / Wens
79	Op het moment dat er nu een video op de vru.nl site wordt geladen vanaf Youtube (ingebed in de pagina) is er een beschermingsconstructie (“Privacy-Enhanced Mode”), waardoor er geen of minimale informatie met Youtube wordt gedeeld over de bezoekers van onze site aan Youtube	Eis
80	De oplossing voldoet aan de Wet digitale toegankelijkheid WCAG 2.1 AA.	Eis

1.8 Authenticatie, autorisaties en vertrouwelijkheden

#	Omschrijving	Eis / Wens
81	De oplossing is in staat autorisaties aan te brengen op minimaal de volgende niveaus: lezen van content, creëren van content, aanpassen van content, publiceren van content en het verwijderen van content.	Eis
82	Het is mogelijk autorisaties en vertrouwelijkheden in te richten per individuele gebruiker, per gebruikersgroep en/of per organisatieonderdeel.	Eis
83	Het systeem heeft een helder rechten- en rollensysteem (toegang en autorisatie). Er moet voor aparte gedeeltes van de site apart lees- en/of schrijfrechten kunnen worden toegekend aan individuele (en groepen) gebruikers of bezoekers. Rechten moeten toegekend kunnen worden aan mensen binnen en buiten de organisatie. Denk hierbij aan medewerkers van gemeenten of partnerorganisaties.	Eis
84	Autorisaties en vertrouwelijkheden voor gebruikers en/of groepen gebruikers zijn door de VRU zelf aan te brengen.	Eis
85	Autorisaties en vertrouwelijkheden maken het mogelijk onderscheid aan te brengen in de mogelijkheden voor gebruikers(groepen) binnen de oplossing. In ieder geval voor de zichtbaarheid van bepaalde metadatavelden, in de getoonde zoekresultaten en in de te nemen acties binnen de oplossing.	Eis
86	Een gebruiker kan meerdere rollen hebben binnen de oplossing. Hij of zij kan toegang hebben tot meerdere vertrouwelijkheden en autorisatieniveaus.	Eis
87	Als de oplossing gebruik maakt van standaard autorisatierollen levert de leverancier een autorisatiematrix op, met daarin de standaardrollen en welke functies die rol mag uitvoeren b.v. invoeren, muteren, publiceren, verwijderen etc.	Eis
88	Aan iedere gebruiker kunnen automatisch basis autorisaties worden toegewezen.	Eis
89	Het is mogelijk specifieke profielen/rollen in te richten voor autorisaties en vertrouwelijkheden.	Eis
90	Voor gebruikers die bekend zijn in de Active Directory van de VRU die toegang zoeken tot de oplossing geldt “single sign-on” (SSO) via ADFS met behulp van SAML2 (SHA-2) of ADFS met behulp van OpenID Connect. Vanaf een VRU-werkplek wordt een gebruiker automatisch ingelogd zonder login prompt.	Eis
91	Autorisaties kunnen door de functioneel-/applicatiebeheerders worden ingesteld, beheerd en gecontroleerd.	Eis
92	Alle functionele beheertaken met betrekking tot de oplossing kunnen worden uitgevoerd terwijl gebruikers zijn ingelogd.	Eis
93	Er kunnen voor de verschillende registratievormen door de beheerder specifieke registraties ingericht worden met eigen metadata. Hier kan dan ook een vaste vertrouwelijkheid op gezet worden.	Eis
94	De oplossing ondersteunt het gebruik van lange en/of complexe wachtwoorden (wachtwoord van minimaal 64 karakters moet mogelijk zijn). Gebruik van speciale tekens is hierbij toegestaan.	Eis
95	De leverancier draagt zorgt voor gebruikersauthenticatie alvorens gebruikers toegang tot de data verkrijgen. Hieronder verstaan wij een gebruikersnaam en sterk wachtwoord, conform het geldende VRU-wachtwoordbeleid.	Eis
96	Binnen de aangeboden oplossing kan de beheerder een overzicht genereren van alle gebruikers met toegekende autorisaties.	Eis

#	Omschrijving	Eis / Wens
97	De oplossing voorziet naast de genoemde SSO methodiek tevens in een alternatieve authenticatiemethode voor gebruikers op basis van een gebruikersnaam en wachtwoord. De mogelijkheid tot afdwingen van sterke wachtwoorden, conform het VRU-wachtwoordbeleid, is aanwezig.	Eis
98	Autorisaties op rollen en andere groepen kunnen genest worden. Dit betekent bijvoorbeeld dat een rol een andere rol kan bevatten. Licht toe hoe dit mogelijk is en geef een voorbeeld.	Wens

1.9 Capaciteit en prestaties

#	Omschrijving	Eis / Wens
99	De oplossing ondersteunt minimaal de aantallen zoals genoemd bij de indicatie van volumes.	Eis
100	Alle interactieve - niet zijnde batchverwerkingen - gebruikersinterfaces van de oplossing voor de gebruikers - zowel intern (medewerkers) als extern - en functioneel beheerders worden in 95% van de gevallen binnen 3 seconden worden getoond. Dit geldt ook voor het tonen van documenten tot 2 MB.	Eis
101	U-Veilig.nl is dynamisch schaalbaar op belasting bij crisis. De site mag niet onderuit gaan bij piekbezoek tijdens een crisis.	Eis
102	De performance van de oplossing dient te allen tijde stabiel te blijven, ongeacht de hoeveelheid opgeslagen data binnen de oplossing.	Eis
103	De hostingcapaciteit is schaalbaar (automatisch op basis van drukte of op aangeven opdrachtgever).	Eis

1.9.1 Onderhoud

#	Omschrijving	Eis / Wens
104	Leverancier verplicht zich om tijdig correctief, perfectief, preventief, adaptief en vernieuwend onderhoud aan de oplossing te plegen. Leverancier verricht alle onderhoud op de oplossing zonder daarvoor kosten in rekening te brengen.	Eis
105	Leverancier verplicht zich tot verbeteren/ vernieuwen / bijhouden van de oplossing naar aanleiding van nieuwe of gewijzigde wet- en regelgeving en landelijke standaarden voor overheden zonder hiervoor extra kosten in rekening te brengen.	Eis
106	De leverancier hanteert een releasekalender en geeft vooraf inzage in de wijzigingen die per toekomstige release worden uitgerold en de invloed ervan op het gebruik van de oplossing door de VRU.	Eis
107	Leverancier houdt de VRU d.m.v. documentatie, bijv. release notes, op de hoogte van uitgevoerde functionele uitbreidingen en wijzigingen van de oplossing.	Eis
108	Leverancier zal voorafgaand aan de implementatie van upgrades, updates en/of andere wijzigingen van de functionaliteit in overleg treden met de VRU, indien deze een verlies van de prestatievermogens van de Saas-dienst en/of verlies van functionaliteit en/of een verminderde beschikbaarheid met zich mee zullen brengen.	Eis
109	Tijdens installatie van de oplossing (ook in de testfase) zijn de handleidingen voor relevante acties die uitgevoerd dienen te worden door de VRU beschikbaar en worden gespecificeerd voor de inrichting van de VRU.	Eis
110	De oplossing wordt geleverd met: • Een functioneel ontwerp/beschrijving, waarin de processen en workflows beschreven zijn voor zowel de front-office-processen als de back-office-processen. • Documentatie van hoofdlijnen/keuzen die zijn gemaakt bij inrichting/configuratie van de oplossing. • Handleidingen voor beheerders.	Eis

#	Omschrijving	Eis / Wens
111	De leverancier levert een beschrijving van de (functionele) tabellen in de database van de oplossing en hun onderlinge relaties (inclusief Database schema) zodat de VRU de gekozen oplossing goed kent en optimaal gebruik kan maken van de oplossing voor bijvoorbeeld rapportages en een eventuele doorontwikkeling naar een BI-tool.	Eis
112	De leverancier stelt gedurende de implementatie en de contractduur, naast de productieomgeving, een acceptatie-omgeving beschikbaar aan de VRU.	Eis

1.10 Ondersteuning

#	Omschrijving	Eis / Wens
113	De leverancier van de oplossing verzorgt een helpdesk, welke als 'single point of contact' dienstdoet voor het stellen van vragen, melden van incidenten en indienen van wijzigingsvoorstellen, alsook voor informatie over de afhandeling daarvan. De helpdesk is telefonisch bereikbaar van 8.00 uur tot 18.00 uur op werkdagen Buiten deze tijden wordt een calamiteitenregeling door leverancier beschikbaar gesteld. In de SLA geeft inschrijver de omgang, respons- en oplostijden aan met aangemelde incidenten. Daarbij wordt tevens de calamiteitenregeling beschreven.	Eis
114	De helpdesk is ook beschikbaar via internet (webportaal of e-mail). Vragen, meldingen van incidenten en wijzigingsvoorstellen kunnen op alle dagen 24 uur per dag online worden ingediend (formulier). Dergelijke online vragen, meldingen van incidenten en wijzigingsvoorstellen worden automatisch per mail bevestigd en daarmee geregistreerd. Tevens kan de voortgang van deze incidenten en wijzigingsmeldingen digitaal worden geraadpleegd en gevolgd.	Eis
115	Van iedere melding is de prioriteit en voortgang zichtbaar. Een melding wordt alleen in overleg met de VRU gesloten.	Eis
116	Leverancier hanteert een prioriteitenmethode of een andere methode waarbij er direct hulp wordt geboden bij incidenten met hoge impact en hoge urgentie, d.w.z. issues waarbij de oplossing niet werkt voor meer dan 1 persoon.	Eis
117	Leverancier verplicht zich ondersteuning te bieden aan de VRU (m.n. functionele beheerders) rondom het beheer en onderhoud van de functionaliteit van de oplossing en de daarin gebruikte bedrijfsinformatie, d.w.z. het instellen van de (functionele) parameters en de inhoud van databases.	Eis
118	Leverancier verplicht zich ervoor te zorgen dat ondersteunende documentatie voor gebruikers en beheerders compleet, correct en up-to-date is.	Eis
119	De leverancier biedt Nederlandstalige opleidingen en opleidingsdocumentatie aan. Deze zijn actueel en gebaseerd op de door de leverancier aangeboden versie van de oplossing. Dit geldt ook bij updates van de oplossing.	Eis
120	De leverancier draagt zorg voor de uitvoering van opleidingen voor de volgende Gebruikers: 1. Functioneel Beheerders 2. Redacteuren	Eis
121	De oplossing dient dusdanig eenvoudig en gebruikersvriendelijk te zijn dat er weinig tot geen opleiding voor een "eindgebruiker" noodzakelijk is. De leverancier biedt voor de eindgebruikers digitale uitleg voor die elementen die ingewikkelder blijken. Dit alles in afstemming met de VRU.	Eis
122	De leverancier staat toe dat de digitale gebruikershandleiding van de oplossing op het interne netwerk van de VRU beschikbaar wordt gesteld of via de oplossing.	Eis
123	De leverancier levert handleidingen en het opleidingsmateriaal op aan functioneel beheerder voor de start van de implementatie.	Eis
124	De leverancier voorziet in een basale eLearning, dan wel in de content voor een eLearning, toegespitst op de meestgebruikte functionaliteiten van de oplossing. Geef hierbij in de toelichting aan wat de leverancier hiervoor kan bieden.	Wens

#	Omschrijving	Eis / Wens
125	De oplossing is bereikbaar via IPv4 en IPv6	Eis
126	Het is voor geautoriseerde beheerders mogelijk om buiten de gebruikersinterface om gegevens te bewerken/bevragen.	Eis

1.11 (Door)Ontwikkeling

#	Omschrijving	Eis / Wens
127	Bij het ontwikkelen en implementeren van nieuwe diensten, producten of componenten geeft de leverancier, voorafgaand aan de daadwerkelijke ontwikkeling en implementatie van wijzigingen per geval, aan of er meerwerk gemoeid is bij het ontwikkelen en implementeren ervan, en of er sprake is van gewijzigde licentiekosten.	Eis
128	Leverancier verplicht zich om de VRU op de hoogte te houden van factoren die van invloed kunnen zijn op de bestaande dienstverlening, als input voor het verder ontwikkelen van de dienstverlening (bijv. nieuwe componenten).	Eis
129	Leverancier houdt de VRU op de hoogte van ontwikkelingen van de dienst, zoals in gebruik bij andere afnemers.	Eis