Information und Technik Nordrhein-Westfalen

IT.NRW · Postfach 10 11 05 · 40002 Düsseldorf

08.12.2023

Aktenzeichen
Z3.02.13.01

Frau Weiß

Durchwahl 0211 9449-6763

Telefax 0211 9449-8075
zentraler-einkauf@it.nrw.de

Elektronische Post

- Ministerium des Innern
- Ministerium für Schule und Bildung
- Ministerium für Wirtschaft, Innovation, Klimaschutz und Energie
- Ministerium für Landwirtschaft und Verbraucherschutz
- Ministerium für Umwelt, Naturschutz und Verkehr
- Ministerium für Arbeit, Gesundheit und Soziales
- Ministerium für Heimat, Kommunales, Bauen und Digitalisierung
- Ministerium für Kinder, Jugend, Familie, Gleichstellung, Flucht und Integration
- Ministerium für Bundes- und Europaangelegenheiten, Internationales und Medien
- Ministerium für Landwirtschaft und Verbraucherschutz
- Ministerium für Kultur und Wissenschaft
- Chef der Staatskanzlei
- Landesrechnungshof
- Landtag
- Landesbeauftragter für Datenschutz und Informationsfreiheit
- Hochschule für Polizei und öffentliche Verwaltung NRW
- Zentralstelle der Länder für Gesundheitsschutz (ZLG)

nachrichtlich

Ministerium der Finanzen

Ministerium der Justiz

IT.NRW
Dienstgebäude
Mauerstraße 51
40476 Düsseldorf
Telefon-Zentrale 0211 9449-01
Telefax 0211 9449-8000
poststelle@it.nrw.de
www.it.nrw.de

Zentraler IT-Einkauf für die Landesverwaltung Nordrhein-Westfalen -Rahmenvertrag über gekapselter Webbrowser -

Der Zuschlag in dem Vergabeverfahren 23-T600423008 wurde erteilt.

Der Rahmenvertrag läuft ab sofort bis maximal zum 14.11.2027.

Den Zuschlag zu der Vergabe ist an die Firma Computacenter AG & Co.oHG, Kokkolastraße 1 in 40882 Ratingen ergangen. .

Nähere Informationen bitte ich dem beigefügten Schreiben zu entnehmen.

Ich bitte Sie, die Dienststellen Ihres nachgeordneten Bereiches über den Vertragsschluss und die Abwicklung über den Einkaufskatalog NRW zu informieren und das beigefügte Schreiben weiterzuleiten.

Im Auftrag
gez. Dr. Koch

Information und Technik Nordrhein-Westfalen

IT.NRW · Postfach 10 11 05 · 40002 Düsseldorf

An alle Bedarfsstellen für IT-Produkte

08.12.2023

Aktenzeichen
Z3.02.13.01

Frau Weiß

Durchwahl 0211 9449-6763

Telefax 0211 9449-8075
zentraler-einkauf@it.nrw.de

Projekt „Einkaufsoptimierung in der Landesverwaltung NRW“
Zentraler IT-Einkauf für die Landesverwaltung Nordrhein-Westfalen
- Rahmenvertrag über gekapselter Webbrowser-

Ich freue mich, Ihnen mitteilen zu können, dass für die nachfolgend aufgeführten Produkte ein neuer Bezugsvertrag abgeschlossen werden konnte:

Gekapselter Webbroswer Vertragsnummer 4600 00 0507

Die Produkte aus diesen Verträgen können ab sofort bis maximal zum 14.11.2027 bezogen werden.

Den Zuschlag erhielt die Firma Computacenter AG & Co.oHG, Kokkolastraße 1, 40882 Ratingen.

IT.NRW
Dienstgebäude
Mauerstraße 51

Administrativer Ansprechpartner ist Herr Paul Ziegner, Tel.-Nr.:+491737238585; Email: paul.ziegner@computacenter.com

Technische Ansprechpartnerin ist Frau Andrea Kehl, Tel.-Nr.:040/30053712 ; Email: mb.presales.wp@computacenter.com

Das vereinbarte Zahlungsziel beträgt 30 Tage nach Eingang einer prüffähigen Rechnung.

Die Produkte können über den elektronischen Einkaufskatalog NRW (http://einkaufskatalog.nrw.de) bestellt werden.

Der o.a. Rahmenvertrag inklusive der Vertragskonditionen werden unter www.vergabe.nrw.de veröffentlicht.

Bei technischen Problemen bitte ich um Mitteilung an kbst-vergabe@fm.nrw.de .

Die Abgeltung der Leistungen des Landesbetriebes IT.NRW nach § 61 Abs. 3 LHO erfolgt durch Rechnungsstellung an die jeweilige Bedarfsstelle in Höhe von derzeit 2% des Jahresbruttoumsatzes der Bedarfsstelle.

Im Auftrag
gez. Dr. Tews

Anlage 1 zum Rahmenvertrag
„Leistungsbeschreibung“

Zentraler IT-Einkauf für die Landesverwaltung Nordrhein-Westfalen

Rahmenvertrag gekapselter Webbrowser

Aktenzeichen Z3.03.02.01
Vergabe Nummer 23-T600423008

Auftraggeber ist das das Land Nordrhein-Westfalen (NRW)

vertreten durch Information und Technik Nordrhein-Westfalen (IT.NRW)

Mauerstraße 51
40476 Düsseldorf

vertreten durch die Betriebsleitung

1 VERTRAGLICHE REGELUNGEN

1.1 Vertragsform und Vertragsbestandteile

Mit Zuschlagserteilung wird ein individueller Rahmenvertrag (Bezugsvertrag) mit einem Wirtschaftsteilnehmer auf Basis der nachstehenden Vertragsbedingungen zwischen dem Land Nordrhein-Westfalen, vertreten durch Information und Technik Nordrhein-Westfalen (IT.NRW), und dem Auftragnehmer geschlossen. Die auf diesen Rahmenvertrag beruhenden Einzelaufträge (Abrufe) werden entsprechend den Bedingungen des Rahmenvertrags vergeben. Der jeweilige Abruf bildet mit diesem Rahmenvertrag einen einheitlichen Vertrag.

Der Vertrag wird in einer besonderen Urkunde („Rahmenvertrag“) dokumentiert.

Als Vertragsform ist ein sogenannter Bezugsvertrag vorgesehen. Die während der Vertragslaufzeit abgerufenen Mengen richten sich ausschließlich nach dem Bedarf des Auftraggebers. Höchstabnahmemengen werden festgelegt.

Der Rahmenvertrag enthält eine Ausschließlichkeitsbindung, d.h. die Bezugsberechtigten verpflichten sich, ihren Bedarf an den ausgeschriebenen Produkten während der Vertragslaufzeit ausschließlich über den Auftragnehmer zu decken.

Es gelten nacheinander als Vertragsbestandteile:

- Rahmenvertrag
- Anlage 1 zum Rahmenvertrag „Leistungsbeschreibung“
- Anlage 2 zum Rahmenvertrag „Leistungskatalog“

- Kostenprofil
- Angebot vom _____
- Besondere vertragliche Nebenbedingung zur Beachtung der in den ILO-Kernarbeitsnormen festgelegten Mindeststandards durch Nachunternehmerinnen bzw. Nachunternehmer unter Berücksichtigung der Vorgaben des Tariftreue- und Vergabegesetzes Nordrhein-Westfalen (TVgG - NRW).
- Ergänzende Vertragsbedingungen für die Überlassung von Standardsoftware gegen Einmalvergütung (EVB-IT Überlassungsvertrag Typ A) AGB in der Version 2.0 Fassung vom 16.07.2015
- Ergänzende Vertragsbedingungen für die Pflege von Standardsoftware AGB (EVB-IT Pflege S) in der Version 2.0 Fassung vom 16.07.2015
- Ergänzende Vertragsbedingungen für die Beschaffung von IT-Dienstleistungen (EVB-IT Dienstleistung) AGB Version 2.1 in der Fassung vom 01.04.2018.
- Allgemeine Vertragsbedingungen für die Ausführung von Leistungen (VOL/B) in der Fassung vom 05.08.2003

Die EVB-IT stehen unter www.cio.bund.de und die VOL/B unter www.vergabe.nrw.de zur Einsichtnahme bereit.
Änderungen oder Ergänzungen an den Vertragsunterlagen sind unzulässig und führen zum Ausschluss des Angebotes von der weiteren Bewertung.
Hinweis:
Dem Angebot dürfen keine allgemeinen Geschäftsbedingungen des Auftragnehmers zu Grunde liegen. Sollten allgemeine Geschäftsbedin-

gungen dem Angebot beiliegen oder auf allgemeine Geschäftsbedingungen des Auftragnehmers verwiesen werden, so wird das Angebot von der weiteren Bewertung ausgeschlossen. Stellen Sie bei Abgabe Ihres Angebots sicher, dass Sie keine allgemeinen Geschäftsbedingungen beigelegt oder darauf verwiesen haben.

1.2 Bezugsberechtigte / Ausschließlichkeitsbindung

Bezugsberechtigt aus dem abzuschließenden Rahmenvertrag sind alle Dienststellen der Landesverwaltung Nordrhein-Westfalen mit Ausnahme des Geschäftsbereichs des Finanzministeriums und Justizministeriums (siehe §§ 3, 6, 7, 8, 9, 14 und 14a Landeorganisationsgesetz NRW).
Die Bezugsberechtigten sind verpflichtet, die ausgeschriebenen Leistungen während der Vertragslaufzeit beim Auftragnehmer zu beziehen. Diese Verpflichtung gilt nicht für Dienststellen, die vertraglich noch an einen anderen Auftragnehmer gebunden sind, für die jeweilige Dauer der noch bestehenden Verträge.
Der Auftragnehmer verpflichtet sich, alle Dienststellen der nachfolgend aufgeführten Ministerien des Landes NRW und deren nachgeordnete Dienststellen während der Vertragslaufzeit zu beliefern:

Ressorts:

- Ministerium des Innern ausgenommen der Bereich Polizei
- Ministerium für Schule und Bildung
- Ministerium für Wirtschaft, Innovation, Klimaschutz und Energie
- Ministerium für Kinder, Jugend, Familie, Gleichstellung, Flucht und Integration
- Ministerium für Arbeit, Gesundheit und Soziales
- Ministerium für Heimat, Kommunales, Bauen und Digitalisierung
- Ministerium für Umwelt, Naturschutz und Verkehr
- Ministerium für Bundes- und Europaangelegenheiten, Internationales und Medien

- Ministerium für Landwirtschaft und Verbraucherschutz
- Chef der Staatskanzlei
- Landtag
- Landesrechnungshof
- Hochschule für Polizei und öffentliche Verwaltung NRW
- Zentralstelle der Länder für Gesundheitsschutz (ZLG)

Es ist nicht ausgeschlossen, dass sich der Zuschnitt der Ressorts während der Vertragslaufzeit ändert.

1.3 Vertragslaufzeit

Die Laufzeit des Rahmenvertrags beginnt mit Zuschlagserteilung. Die Mindestvertragsdauer beträgt 12 Monate. Der Vertrag verlängert sich automatisch jeweils um weitere 12 Monate, wenn er nicht schriftlich mit einer Frist von 3 Monaten vor Ablauf der Vertragsdauer von einem der beiden Vertragspartner gekündigt wird. Der Vertrag läuft maximal 48 Monate ab Vertragsbeginn. Die Kündigung des Rahmenvertrages oder dessen sonstige Beendigung berührt nicht die Wirksamkeit des bereits getätigten Abrufs. Für innerhalb der Vertragslaufzeit getätigte Abrufe bleiben die Bedingungen dieses Rahmenvertrages auch nach dessen Beendigung oder Kündigung bestehen.

1.4 Schätzung der Auftragswerte /Höchstmenge

Vor der Erstellung der Vergabeunterlagen wurde eine landesweite Bedarfsabfrage über die Produkte durchgeführt. Die bezugsberechtigten Dienststellen wurden aufgefordert, ihren geschätzten Bedarf für die Jahre 2023 bis einschließlich 2026 zu benennen. Die auf diese Weise ermittelten Mengen stellen die geschätzten Abnahmemengen dar.
Es werden keine Mindestabnahmen aus diesem Vertrag garantiert.
Es besteht kein Anspruch auf Erreichen des geschätzten Gesamtauftragswertes. Das Erreichen oder die Überschreitung des geschätzten Gesamtauftragswertes beendet diesen Vertrag nicht.

Der Auftragnehmer verpflichtet sich, unabhängig von der angeforderten Menge zu den in diesem Vertrag vereinbarten Regelungen zu leisten.
Während der Laufzeit dieses Vertrages ist der Auftraggeber verpflichtet, die zugrunde gelegten Leistungen über diesen Vertrag zu beziehen.
Das geschätzte Auftragsvolumen beträgt: 2.100.000 €/netto
Die Höchstmenge beträgt 3.150.000 €/netto.
Der auf diese Weise ermittelte geschätzte Auftragswert stellt die geschätzte Abnahmemenge dar. Eine Mindestabnahme von Leistungen aus diesem Vertrag wird nicht garantiert.
Die maximale Vertragslaufzeit endet 48 Monate nach Vertragsbeginn bzw. endet bei Erreichen der Höchstmenge ohne dass es einer Kündigung bedarf, je nachdem, welches Ereignis früher eintritt

1.5 Bestellungen/Einkaufskatalog

Die Bestellungen aus diesem Rahmenvertrag werden nach folgendem Verfahren durchgeführt:
Der Abruf von Leistungen erfolgt direkt durch die Bezugsberechtigten auf Grundlage des Rahmenvertrags über den Einkaufskatalog NRW.
Um die Bestellung über den Einkaufskatalog NRW abwickeln zu können, ist der Auftragnehmer verpflichtet, die Produktdaten zu den vertraglich vereinbarten Produkten für den Import im Format Excel oder als csv. Datei zur Verfügung zu stellen.
Erstmalig spätestens fünf Tage nach Zuschlagserteilung sind diese Daten dem Auftraggeber im vg. Format elektronisch zur Verfügung zu stellen.

Der Auftragnehmer ist verpflichtet, die Bestellung elektronisch per E-Mail entgegenzunehmen und sie im gleichen Format innerhalb eines Arbeitstages (Mo-Fr) zu bestätigen. Eine Muster-Email, aus der das Format der Bestellung ersichtlich ist, liegt als Anlage: Anlage 1.1 Musterbestellung den Ausschreibungsunterlagen bei.

Mit dem Abruf durch die jeweilige Bezugsberechtigte Dienststelle gehen die vertraglichen Rechte und Pflichten des Auftraggebers auf die abrufende Dienststelle über.

Die Lieferung bzw. Lizenzierung der Produkte erfolgt durch den Auftragnehmer direkt an die jeweilige Behörde oder Einrichtung des Landes NRW. Die Lieferung und Rechnungsstellung der angebotenen Leistung erfolgt unmittelbar an den jeweiligen Abnehmer soweit nichts Anderes im Abruf angegeben wird.

1.6 Lieferung der Produkte

Die Lieferung der Lizenzen muss spätestens 14 Tage nach Abrufeingang erfolgen. Die Lieferung der angeforderten Produkte erfolgt frei Verwendungsstelle, entweder als elektronische Zustellung an die bestellenden Dienststellen des Landes NRW oder als Bereitstellung zum Download im Internet über die Seite des Auftragnehmers oder des Herstellers.

Der Auftraggeber kann den Vertrag kündigen, wenn die Lieferzeit mehr als zweimal innerhalb eines halben Jahres nicht eingehalten wird.

1.7 Vergütung / Vergütungsvorbehalt

Die jeweiligen in der Anlage 5 zum Rahmenvertrag „Kostenprofil“ angegebenen Preise (Einzelpreise) sind netto und in Euro anzugeben.

Diese Preise können frühestens 12 Monate nach Vertragsschluss erhöht werden. Weitere Erhöhungen können frühestens nach Ablauf von jeweils 12 Monaten gefordert werden. Eine Erhöhung ist dem Auftraggeber anzukündigen und wird frühestens 3 Monate nach Zugang der Mitteilung wirksam. Voraussetzung für die Wirksamkeit ist, dass der Auftragnehmer die Vergütung als allgemeinen Listenpreis vorsieht und auch von anderen Auftraggebern erzielt.

Sind die Voraussetzungen für eine Erhöhung der Vergütung erfüllt, hat der Auftraggeber innerhalb der Ankündigungsfrist das Recht, den Vertrag ganz oder nur für die von der Erhöhung betroffenen Leistungen (einzelne Produkte) frühestens zum Zeitpunkt des In-Kraft-Tretens der

neuen Preise zu kündigen, sofern die Erhöhung 3 % der zuletzt gültigen Preise überschreiten sollte.

Bei Preisminderungen innerhalb der Vertragslaufzeit sind diese sofort an den Auftraggeber weiterzugeben. Der Auftraggeber behält sich vor, in regelmäßigen Abständen eine Marktanalyse zur Preiskontrolle durchzuführen. Sollten die Produkte am Markt wesentlich wirtschaftlicher (mindestens 5 % niedriger) zu beschaffen sein, kann der Auftraggeber fristlos ganz oder teilweise vom Vertrag zurücktreten.
Dieser Vergütungsvorbehalt gilt auch für die Pflegevergütung.

1.8 Rechnungsstellung

Die Rechnungsstellung für den Abruf von Lizenzen erfolgt einmalig nach Lieferung und ist zahlbar 30 Tage nach Eingang einer prüffähigen Rechnung bzw. 14 Tage nach Eingang einer prüffähigen Rechnung unter Abzug von Skonto.

Die Rechnungsstellung für die EVB-IT Pflegeverträge erfolgt jährlich im Voraus.

Die Rechnungsstellung für die erbrachten Dienstleistungen (Personentage) erfolgt gem. Ziffer 6.1 EVB-IT Dienstleistung kalendermonatlich nachträglich für die tatsächlich erbrachten Leistungen und ist zahlbar 30 Tage nach Eingang einer prüffähigen Rechnung bzw. 14 Tage nach Eingang einer prüffähigen Rechnung unter Abzug von Skonto.

Die Rechnungsstellung für den jeweiligen Abruf erfolgt nach Lieferung direkt gegenüber der zu beliefernden Dienststelle. Rechnet die Dienststelle nicht selbst ab, so benennt sie die abrechnende Dienststelle in dem Abruf.
Für den Auftraggeber (IT.NRW) gilt: Um eine reibungslose Rechnungsabwicklung gewährleisten zu können, müssen alle Dokumente, insbesondere Rechnungen, Lieferscheine und Leistungsnachweise zu einem Abruf die EK-Bestellnummer, die Rahmenvertragsnummer und, wenn

vorhanden, auch die Kundenauftragsnummer aufweisen. IT.NRW behält sich vor, Rechnungen, die aufgrund fehlender Angaben nicht bearbeitet werden können, zurückzuweisen.
Der Auftragnehmer leitet dem Auftraggeber alle relevanten Angaben (auch der Lizenzgeber) weiter.

1.9 Reports

Der Auftragnehmer hat dem Auftraggeber auf Anforderung einen Report in elektronischer Form zur Verfügung zu stellen. Dieser Report soll an die E-Mail-Adresse sourcing-leadbuyer@it.nrw.de gesendet werden und mindestens folgende Angaben enthalten:
Produktbezeichnung, Produktnummer, Seriennummer, Anzahl der abgerufenen Produkte, Nettopreis, Bestell- und Lieferdatum, Laufzeit der Pflegeverträge sowie die Abrufscheinnummer.

1.10 Datenschutz, Datensicherheit, Vertraulichkeit

1.10.1 Der Auftraggeber sorgt dafür, dass dem Auftragnehmer alle relevanten, über die gesetzlichen Regelungen hinausgehenden Sachverhalte, deren Kenntnis für ihn aus Gründen des Datenschutzes und der Geheimhaltung erforderlich ist, bekannt gegeben werden.
1.10.2. Vor Übergabe eines Datenträgers an den Auftragnehmer stellt der Auftraggeber die Löschung schutzwürdiger Inhalte sicher, soweit nichts anderes vereinbart ist.
1.10.3. Der Auftragnehmer sorgt dafür, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung des Vertrages betraut sind, die gesetzlichen Bestimmungen über den Datenschutz beachten. Die nach Datenschutzrecht erforderliche Verpflichtung auf das Datengeheimnis ist spätestens vor der erstmaligen Aufnahme der Tätigkeit vorzunehmen und dem Auftraggeber auf Verlangen nachzuweisen.
1.10.4. Der Auftraggeber kann den Vertrag ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten nach Ziffer 1.10.3 unter Berücksichtigung der Sachverhalte gemäß Ziffer 1.10.1 schuldhaft in-

nerhalb einer gesetzten angemessenen Frist nicht nachkommt oder Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt.

1.10.5. Der Auftragnehmer darf grundsätzlich nicht auf personenbezogene Daten zugreifen, die der Auftraggeber verarbeitet. Abweichend hiervon ist dem Auftragnehmer gestattet, zur Erfüllung seiner vertraglichen Verpflichtungen auf personenbezogene Daten zuzugreifen.
Der Auftragnehmer ist nicht befugt, Daten des Auftraggebers für eigene oder für Zwecke Dritter zu verwenden.
1.10.6. Soweit der Auftragnehmer Dritte zur Erfüllung von Leistungen aus diesem Vertrag (nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber zulässig) heranzieht, hat er diese und etwaige Subunternehmer zur Einhaltung der in diesem Vertrag enthaltenen datenschutzrechtlichen Bestimmungen zu verpflichten; dazu gehört insbesondere das Kontrollrecht der Landesbeauftragten für den Datenschutz gegenüber dem Dritten bzw. dem Subunternehmen.
1.10.7. Auftraggeber und Auftragnehmer sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten vertraulichen Informationen, Geschäfts- und Betriebsgeheimnisse strikt vertraulich zu behandeln, insbesondere nicht an Dritte weiterzugeben oder sonst zu verwerten. Dies gilt auch für den Erfahrungsaustausch innerhalb der öffentlichen Hand.
Vertrauliche Informationen im Sinne dieser Vereinbarung sind:

- Alle mündlichen oder schriftlichen Informationen und Materialien, die der Auftragnehmer direkt oder indirekt von IT.NRW zur Abwicklung des Auftrages erhält und als vertraulich gekennzeichnet sind oder deren Vertraulichkeit sich aus ihrem Gegenstand oder sonstigen Umständen ergibt.
- Die beauftragten Leistungen und sonstige Arbeitsergebnisse.

Der Auftragnehmer wird alle geeigneten Vorkehrungen treffen, um die Vertraulichkeit sicherzustellen. Vertrauliche Informationen werden nur

an die Mitarbeiterinnen/Mitarbeiter weitergegeben, die sie aufgrund ihrer Tätigkeit erhalten müssen.
Die Pflicht zur absoluten Vertraulichkeit dauert auch nach Beendigung der Zusammenarbeit an. Auf Verlangen sind ausgehändigte Unterlagen einschließlich aller davon angefertigten Kopien sowie Arbeitsunterlagen und -materialien zurückzugeben.

Dies gilt auch über die Vertragslaufzeit hinaus.
1.10.8. Die Verpflichtung gilt auch für die Rechtsnachfolger der Parteien. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

- Der Auftraggeber sorgt dafür, dass dem Auftragnehmer alle relevanten, über die gesetzlichen Regelungen hinausgehenden Sachverhalte, deren Kenntnis für ihn aus Gründen des Datenschutzes und der Geheimhaltung erforderlich ist, bekannt gegeben werden.

1.10 Umsetzung der Empfehlungen des BSI für die Handhabung von Schwachstellen

Der Auftragnehmer verpflichtet sich, die Empfehlungen des BSI für die Handhabung von *Schwachstellen* umzusetzen. Ist dem Auftragnehmer der Einsatz von Unterauftragnehmern gestattet oder bezieht er Software* von einem Zulieferer oder dem Hersteller selbst, muss er diese so auswählen, dass die Umsetzung der Empfehlungen des BSI durch diese oder den Auftragnehmer selbst gewährleistet ist.

- Die Verpflichtung gemäß dieser Nummer 1.10 bezieht sich ausschließlich auf vertragsgegenständliche Individualsoftware sowie die vertragsgegenständlichen Anpassungs- bzw. Customizingleistungen, nicht jedoch auf die Standardsoftware*.

- Die Verpflichtung gemäß dieser Nummer 1.10 bezieht sich ebenfalls auf vom Auftraggeber beigestellte Software*, soweit diese im Quellcode* übergeben wurde.

1.11 Mängelhaftung (Gewährleistung)

Ergänzend zur Mängelhaftung gewährleistet der Auftragnehmer, dass die vertragsgegenständliche Software* frei von vermeidbaren Schwachstellen ist. Dazu zählen mindestens die in den jeweils aktuellen Ausgaben der SANS Top 25 (Quelle: SANS TOP25) (oder entsprechenden Nachfolgern) und im Fall von Web-Anwendungen auch der OWASP Top 10 (oder entsprechenden Nachfolgern) aufgeführten Schwachstellentypen.

- Der Auftragnehmer hat zu diesem Zweck bereits im Design-, Entwicklungs- und Testprozess der Software entsprechende Maßnahmen ergriffen und führt diese im Rahmen seiner Produktbeobachtung, der. Pflege sowie bei der Weiterentwicklung laufend fort.

- Ist der Auftragnehmer nicht selbst Hersteller, wählt er nur Produkte solche Hersteller aus, die dargelegt haben, dass sie entsprechende Maßnahmen ergriffen haben und laufend fortführen.

- Auf Verlangen des Auftraggebers wird der Auftragnehmer die ergriffenen Maßnahmen und ihre Effektivität gegenüber dem Auftraggeber umfassend darstellen.

Auftragsgegenstand

Die vorliegende Leistungsbeschreibung hat die Implementierung eines gekapselten Browsers sowie begleitender Services für eine maximale Vertragslaufzeit von vier Jahren zum Gegenstand.

2.1 Informationen zum Mengengerüst

Hierzu wurde eine Bedarfsabfrage im Land durchgeführt, über die potentielle Interessenten identifiziert und deren Mengengerüst abgefragt wurden.
Dadurch kommt folgende Abschätzung zu Stande ca. .

	Lizenzen (pro Client)
Behörden und Einrichtungen der Landesverwaltung NRW	30.000

2.2 Zielsetzung der Ausschreibung

Mit der Auswahl und Einführung einer im vorliegenden Dokument beschriebenen Lösung werden die folgenden Ziele verfolgt:

- Das übergeordnete Ziel ist die Erhöhung der IT-Sicherheit durch Verringerung der Risiken, die durch das Surfen im Internet entstehen.
- Es soll eine gekapselte Webbrowser-Lösung angeschafft werden, damit potentiell gefährliche Inhalte aus dem Internet in einer kontrollierten Umgebung verbleiben und keinen Schaden in der IT-Umgebung erzeugen können.
- Die Anwenderinnen und Anwender sollen mit der gekapselten Webbrowser-Lösung möglichst keine Einschränkungen bei der täglichen Arbeit sowie im Umgang mit dem Webbrowser haben.
- Die Client-Rechner der Anwenderinnen und Anwender sowie das angeschlossene Netzwerk sollen vor Exploits, CSRF, XSS, Trojanern, Würmer, Viren, Ransomware etc. geschützt werden.

- Im Falle eines Befalls durch Schadsoftware muss der Schaden innerhalb der gekapselten Webbrowser-Lösung verbleiben und darf das Clientsystem oder Netzwerk nicht gefährden.
- Die gekapselte Webbrowser-Lösung muss derart gestaltet sein, dass eine zentralisierte Administration sowohl der Konfiguration als auch der Softwarebestandteile ermöglicht wird.
- Die gekapselte Webbrowser-Lösung soll außerdem Funktionen bereitstellen, die eine Analyse einer befallenen, gekapselten Webbrowser-Umgebung ermöglicht, sodass ggf. weitere vorbeugende Maßnahmen möglich sind.
- Es muss für die Anwenderinnen und Anwender die Möglichkeit geben, individuelle Browser-Einstellungen, Favoriten oder RSSFeeds. zu speichern, sodass diese bei erneutem Start der Lösung zur Verfügung stehen.
-

Weiterhin bedarf es der Möglichkeit, der Übergabe von heruntergeladenen Inhalten aus der gekapselten Webbrowser-Lösung in der Client-Umgebung der Anwenderrinnen und Anwender. Hierbei muss die Sicherheit auf dem Client durch Maßnahmen z.B. Scan der Inhalte auf Schadcode) auf dem Hostsystem aufrechterhalten werden.

Eignungskriterien an Unternehmen

Die Eignung der Bieter wird anhand der Leistungsfähigkeit, der Fachkunde und der Zuverlässigkeit bewertet. Hierfür werden die nachfolgenden Kriterien zu Grunde gelegt. Die Anforderungen sind hier im Überblick aufgelistet. Entsprechende Auskünfte sind durch die Bieter in der Anlage 2 „Leistungskatalog“ sowie durch entsprechende Nachweise zu tätigen.

Erfahrungen am Markt

Der Anbieter muss über mindestens drei Jahre Erfahrung im Marktbereich der gekapselten Browser verfügen (dies ist durch entsprechende Referenzen nachzuweisen)

Referenzen

Belegen Sie ihre Erfahrung mit der Implementierung von gekapselten Browsern in vergleichbarer Ausprägung hinsichtlich Leistungsgegenstand, Größenordnung/Volumen und Scope auf Basis von drei geeigneten Referenzen zu vergleichbaren Auftraggebern (vorzugsweise Behör-

den, Ministerien, Justiz). Unter vergleichbaren Auftraggebern sind zu verstehen: Behörden mit mehr als 3.000 Mitarbeitern/physischen Clients, Behörden mit mehr als 3.000 Mitarbeitern/physischen Clients oder Firmen an mehreren Standorten mit mehr als 3.000 Mitarbeitern/physischen Clients. Hierbei sind die Kontaktpersonen zu benennen, die ggf. für Rückfragen bereitstehen. Zudem ist Art und Umfang des jeweiligen Projekts in Bezug auf die vorstehenden Anforderungen an die Vergleichbarkeit kurz zu beschreiben.

Deutschsprachige Hotline

Der Anbieter muss zur allgemeinen Unterstützung des Betriebs eine deutschsprachige Hotline betreiben, über die entsprechende Anfragen berechtigter User und Admins eingereicht und beantwortet werden können. Der Auftragnehmer gewährt dem Auftraggeber zu folgenden Zeiten die Möglichkeit zur unmittelbaren telefonischen Kontaktaufnahme zu Sicherheitsexperten. Diese Hotline muss montags bis freitags (außer an Feiertagen am Erfüllungsort) von 8:00 bis 17:00 Uhr erreichbar sein.

Weitere Anforderungen sind unten aus 2.4 „Anforderungen an die Transparenz & Kommunikation zu entnehmen“.

Betrieb eines Testsystems

Der Anbieter muss zur allgemeinen Unterstützung des Auswahlverfahrens und zur späteren Unterstützung bei der Evaluierung der Lösung sowie neuer Versionen und/oder Funktionen vor Ort unterstützen.

Allgemeine Anforderungen

Im folgenden Kapitel sind allgemeine, übergreifende Anforderungen an die anzubietende Leistung aufgeführt. Die Erfüllung der Anforderungen wird zum einen im Rahmen der Buchbewertung der Angebote (siehe Anlage „Bewertungsschema“) wie auch in der Teststellung (siehe Hinweise zur Teststellung im laufenden Text) vom Auftraggeber überprüft und bewertet.

Der Anbieter muss im Rahmen der Systemimplementierung und der darauffolgenden individuellen Unterstützung während der Vertragslaufzeit den jeweiligen Kunden Unterstützung anbieten. Die Systemimplementierung muss ebenfalls durch den Auftragnehmer vor Ort angeboten werden.

2.4 Anforderungen an die Transparenz & Kommunikation

Aus Gründen der Planungssicherheit auf Seiten des Auftraggebers muss der Anbieter der Lösung die zukünftige Entwicklung der Lösung und darin enthaltener Bestandteile transparent und offen beschreiben sowie dies an den Auftraggeber kommunizieren. Dies bedeutet, dass z. B. Entscheidungen über Änderungen beim zukünftigen Funktionsumfang einer neuen Version rechtzeitig, d.h. mit einem Vorlauf von mindestens 4 Wochen, sowie grundlegende Meilensteinentscheidungen, d.h. z. B. Abkündigung der Lösung oder Bestandteile darin, Ende des Verkaufs weiterer Lizenzen / Erweiterbarkeit usw., mit einem Vorlauf von mindestens 6 Monaten dem Auftraggeber durch den Anbieter aktiv, z. B. durch ein Schreiben, mitgeteilt werden.

Insofern innerhalb der IT des Anbieters durch Angriffe, Sabotage und andere Formen der Verdacht besteht oder derlei erfolgreich war, dass Daten über den Auftraggeber entwendet wurden, dann ist der Anbieter dazu verpflichtet, den Auftraggeber unverzüglich über Art und Umfang der Datenentwendung zu informieren. Unverzüglich heißt, nach Kenntnis telefonisch die Entwendung zu melden sowie im Nachgang schriftlich Art, Umfang, durchgeführte Sofortmaßnahmen sowie Maßnahmen zur langfristigen Absicherung mitzuteilen.
Schwachstellen im Sinne des Vertrages sind, in Anlehnung an die Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI),

sicherheitsrelevante Fehler von Software* bzw. eines IT-Systems. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und ein System geschädigt wird. Durch eine Schwachstelle wird ein System anfällig für Bedrohungen. Schwachstellen in Hard- oder Software sind Mängel.

Mitigation bezeichnet eine kompensierende Sicherheitsmaßnahme in Form einer vorübergehenden Absicherung einer Schwachstelle bzw. einer erheblichen Milderung des damit verbundenen Risikos, bis eine ursächliche Fehlerbehebung zur Verfügung steht.

Vorrang von Bestimmungen zu Schwachstellen

Liegt eine Schwachstelle vor, so haben die schwachstellenspezifischen Bestimmungen in diesem Vertrag Vorrang gegenüber den sonstigen Bestimmungen, soweit diese nicht weitergehende Rechte des Auftraggebers enthalten.

Behebung von Schwachstellen

Während der Verjährungsfrist für Mängelansprüche, unabhängig davon aber mindestens während der gesamten Laufzeit der Pflege ist der Auftragnehmer unverzüglich und ohne gesonderte Vergütung zur Behebung von *Schwachstellen* durch vollständige Beseitigung ohne Funktionseinbußen verpflichtet, Dies gilt auch für Leistungen bzw. Software* seiner Unterauftragnehmer und Zulieferer. Bis zur ursächlichen Behebung stellt der Auftragnehmer Möglichkeiten zur *Mitigation* zur Verfügung.

Die anwendbaren Fristen für die Behebung von *Schwachstellen* richten sich nach der jeweiligen Kritikalität der *Schwachstelle*. Diese wird mithilfe des Common Vulnerability Scoring System (CVSS) in der jeweils aktuellen Version bewertet. Es gilt im Zweifelsfall die Bewertung des Auftraggebers.

Es werden folgende Fristen vereinbart:

Kritikalität	CVSS Base Score	*Mitigation*	Vollständige Behebung der *Schwachstelle* ohne Funktionseinbußen
Kritisch	9.0 bis 10.0	innerhalb 72 Stunden	binnen 30 Werktagen
Hoch	7.0 bis 8.9	binnen 5 Werktagen	
Mittel	4.0 bis 6.9	binnen 5 Werktagen	binnen 60 Werktagen
Niedrig	Kleiner 4.0	ohne Vorgabe	binnen 90 Werktagen

Die vorgenannten Fristen laufen ab dem Zeitpunkt des öffentlichen Bekanntwerdens oder ab dem Zeitpunkt der Mitteilung durch den Auftraggeber oder eines Dritten, je nachdem, welcher Zeitpunkt früher ist.
Ein Fristaufschub für die Beseitigung der *Schwachstelle* kann in Ausnahmefällen schriftlich gewährt werden, sofern der Auftragnehmer aus nachvollziehbaren technischen Gründen an der fristgemäßen Beseitigung der *Schwachstelle* gehindert ist.

2.5 Anforderungen an die EVB-IT Pflege/Support Leistungen

Die Leistung wird gegen pauschale Vergütung vereinbart.

Der Auftragnehmer erbringt für den Auftraggeber die folgenden Pflegeleistungen:

Im Falle von Produktstörungen wird eine Reaktionszeit von 24 Stunden und eine Wiederherstellungszeit von 5 Werktagen (Mo.-Fr.) vereinbart.
Die Leistung muss, wenn nötig, auch vor Ort bei den Kunden erfolgen.
Für die vollständige Vertragsdauer muss der Auftragnehmer werktags (Mo.-Fr.) innerhalb der üblichen Geschäftszeiten von 08:00-17:00 Uhr für Problem- und Störungsmeldungen telefonisch (Hotline) und elektronisch erreichbar sein. Eine fernmündliche Störungsmeldung reicht aus.

Die Hotline muss in der o.g. Zeit ständig erreichbar sein. Die Hotline sollte mindestens nach Name, Behörde und Fehler fragen. Falls eine telefonische Behebung des Fehlers nicht möglich ist, sollte der Zeitpunkt für die Rücksendung verbindlich festgelegt oder der Termin für die Behebung mit dem Anrufer vereinbart und per E-Mail unter Angabe des Störungseingangs bestätigt werden. Sollte eine direkte Terminfestlegung nicht möglich sein, ist der Anrufer unmittelbar nach Festlegung des Termins zu informieren. Dabei sind die Reaktionszeiten und die Terminwünsche des Auftragsgebers zu beachten. zusätzlich ist die Verfügbarkeit der E-Mail-Funktion für die Störungsmeldungen einzurichten.

Basispflegeleistung

Bereitstellung verfügbarer Umgehungen, Patches und Updates. Unverzüglich sobald vom Hersteller freigegeben. Art der Lieferung: Bereitstellung im Internet zum Download.

Lieferung von Upgrades*, Releases*/Versionen*

Bereitstellung verfügbarer Upgrades und Releases/Versionen ohne Verpflichtung bezüglich Häufigkeit und Umfang. Unverzüglich sobald vom Hersteller freigegeben. Art der Lieferung: Bereitstellung im Internet zum Download.

3 FUNKTIONALE ANFORDERUNGEN AN DAS TOOL

Im folgenden Kapitel erfolgt die Definition der vom Auftraggeber geforderten fachlichen Funktionen. Die Erfüllung der Anforderungen wird zum einen im Rahmen der Buchbewertung der Angebote wie auch in der Produktdemo vom Auftraggeber überprüft und bewertet. (Details siehe Anlage „Leistungskatalog gekapselter Browser“).

3.1 Kernfunktionen

3.1.1 Browser

Die gekapselte Webbrowser-Lösung muss einen Zugriff auf vom Auftraggeber nicht gesperrte Webseiten über vorhandene Proxys des Auftraggebers und den dortigen Auf-und Abruf entsprechender Webinhalte ermöglichen. Der eingesetzte Browser muss einem aus der Top 3 in Deutschland im Einsatz befindlichen Webbrowser entstammen. Diese entsprechen im Jahr 2023 folgenden Produkten[1]: Mozilla Firefox, Google Chrome und Microsoft Edge.

3.1.2 Aktualität des Browsers

Die Lösung muss derart gestaltet sein, dass der implementierte Browser in regelmäßigen Abständen in Form von Updates/Upgrades zur Implementierung in die gekapselte Umgebung zur Verfügung steht. Als Quelle für die Updates/Upgrades dienen die offiziellen Releases des jeweiligen Browserherstellers. Die Sicherheit des eingesetzten Browsers muss gewährleistet werden. Der vorgegebene Updatezyklus ist als Nachweis dem Angebot beizufügen.
Nach Bekanntwerden von schwerwiegenden, d.h. gravierenden Sicherheitslücken im implementierten Browser, die einen uneingeschränkten Weiterbetrieb nicht mehr ermöglichen, muss nach gemeinsamer Absprache zwischen Auftraggeber und Auftragnehmer auch außerhalb des

vorgegebenen Updatezyklus ein entsprechendes Update/Upgrade bereitgestellt werden. Unter schwerwiegenden Sicherheitslücken werden Schwachstellen wie z.B. die SSL-Schwachstelle in 2023 oder vom Schweregrad damit vergleichbare Schwachstellen wie z.B. das Ausführen von Schadcodes gemeint. Solche Schwachstellen werden in der Regel durch das BSI und andere Medien (z.B. Heise / Heise Security und tecchannel) mit entsprechen hoch kritischen Risikoeinschätzungen kommuniziert. Eine einvernehmliche Risikoabschätzung zwischen Auftraggeber und Auftragnehmer ist erforderlich. Der Auftraggeber verpflichtet sich, in solchen Fällen auch außerhalb des regulären Updatezyklus entsprechende Updates bereitzustellen.

3.1.3 Schutz gegen Bedrohungen

Die gekapselte Webbrowser-Lösung sollte auch innerhalb der Umgebung einen Schutz vor Exploits, CSRF, XSS, Trojanern, Würmer, Viren, Ransomware, Makro Viren, Schadecodes und anderen Bedrohungen (Emotet) implementieren. Die Sicherheitsfeatures des eingesetzten Browsers selber dürfen durch die Lösung nicht eingeschränkt werden. Hierbei sollten auch die BSI Anforderungen eingehalten werden. (z.B. BSI Ransomware Maßnahme Katalog)

3.1.4 Abschottung von Angriffen / Angriffsversuchen

Angriffsversuche und/oder erfolgreiche Angriffe müssen getrennt innerhalb der gekapselten Webbrowser-Lösung verbleiben. Es darf keine Auswirkungen auf das Client-System der Anwenderinnen und Anwender und dem Netzwerk geben.

3.1.5 Protokollierung sicherheitsrelevanter Ereignisse

Die gekapselte Webbrowser-Lösung zeichnet sicherheitsrelevante Ereignisse im Zusammenhang mit Schadsoftware derart auf, dass eine forensische Untersuchung und technische Analyse der Ursachen er-

möglicht wird. Die Protokollierung muss[2] derart gestaltet sein, dass nur ein berechtigter Personenkreis (z.B. Administratoren) mit entsprechenden Hinweismeldungen Zugriff auf potentiell gefährliche Inhalte erhält. Eine Export-Funktion der Protokollierung ist erforderlich, um entsprechende Analysen in separaten Umgebungen des Auftraggebers oder anderer Stellen durchführen zu können. Benutzerverhalten darf nicht protokolliert werden.

3.1.6 Zentrale Administration

Die gekapselte Webbrowser-Lösung muss eine zentralisierte Management-Plattform mit Webinterface zur Verfügung stellen, über die sämtliche administrativen Arbeiten erfolgen. Hierzu zählen insbesondere die Verwaltung von Updates/Upgrades, Konfiguration, definieren der Policies und die Protokollierung/Logging.
Die vom Auftragnehmer bereitzustellende Lösung muss so konzipiert sein, dass ihr Einsatz für den Auftraggeber ohne weitere Investitionen (z.B. Folgekosten für Datenbanken) möglich ist. Der Angebotspreis bezieht sich somit auf eine betriebsbereite gekapselte Webbrowser-Lösung inklusive gegebenenfalls nötiger oder vom Hersteller empfohlener Verwaltungswerkzeuge.

3.1.7 Active Directory

- Das Produkt sollte innerhalb einer Active Directory Domänen Struktur kompatibel sein.
- Die vollständige Benutzer-/Gruppenverwaltung kann über das Active Directory verwaltet werden.

Potentiell gefährliche Dateien dürfen nicht als ausführbarer Code auf Servern innerhalb des IT.NRW- bzw. Kunden-Netzes gespeichert werden, sondern z.B. in einem Quarantäneordner.

3.1.8 Rollen- und Rechtekonzept der Administration

Die Management-Plattform sollte ein entsprechendes Rollen- und Berechtigungskonzept zur Verfügung stellen. Die folgenden vier Rollen werden hierbei erwartet:

- Voll-Administrator: Vollzugriff auf alles
- Rollout-Administrator: Verwaltung der Updates/Upgrades
- Policies-Administrator: Verwaltung der Konfigurationen und Policies
- Analyst: lesender Zugriff auf Rollout- und Policies-Bereich, Vollzugriff auf Protokollierung /Logging

3.1.9 Kompatibilität mit Softwareverteilung z.B. SCCM

Die Installation sollte mit Microsoft SCCM möglich sein. Sie sollte auch mit anderen MSI-basierenden Softwareverteilungsprodukten kompatibel sein. Die Software muss nach Installation uneingeschränkt mit Benutzerrechten zu betreiben sein.
Die Software muss den Qualitätsanforderungen des Herstellers Microsoft für Installationen auf dem jeweiligen Betriebssystem genügen.
Die Lösung muss nach Installation uneingeschränkt mit Benutzerrechten zu betreiben sein.

3.1.10 Standort der Lösung „keine Cloud Variante“

Die gesamte Lösung muss im Netz des Auftraggebers betrieben werden. Es darf keine ausgelagerten Komponenten / Funktionen geben.

3.1.11 Zeitkritische Anwendungen

Die gekapselte Webbrowser-Lösung muss zeitkritische Webinhalte (z. B. Streaming, Chat, Videokonferenzen und Portal Zugänge) ohne Qualitätsverlust und ohne für die Anwenderinnen und Anwender spürbare Verzögerung darstellen können. Die Sicherheit gemäß 3.1.4 ist hierbei auch sicherzustellen.

3.1.12 Übergabe von Inhalten zwischen Client und gekapselter Umgebung

Es muss für Anwenderinnen und Anwender möglich sein, heruntergeladene Inhalte aus dem Internet auf den Client zu übertragen. Hierbei muss die Schnittstelle zwischen der gekapselten Webbrowser-Lösung und dem Client den Inhalt mit dem auf dem Host installierten Virenscanner oder einem sich täglich automatisch aktualisierendem integriertem Virenscanner auf Schadcode überprüfen. Weiterhin wird erwartet, dass Anwenderinnen und Anwender Inhalte vom Client über die gekapselte Webbrowser-Lösung in das Internet übertragen können.

3.1.13 Zwischenablage

Die Zwischenablage muss zur Übertragung von Texten und Bildern aus dem Internet über die gekapselte Webbrowser-Lösung auf den Client zur Verfügung stehen. Hierbei muss die Schnittstelle zwischen der gekapselten Webbrowser-Lösung und dem Client den Inhalt mit dem auf dem Host installierten Virenscanner oder einem sich täglich automatisch aktualisierendem integriertem Virenscanner auf Schadcode überprüfen. Weiterhin wird erwartet, dass Anwenderinnen und Anwender die Zwischenablage vom Client über die gekapselte Webbrowser-Lösung im Internet nutzen können.

3.1.14 Persistente Speicherung von Einstellungen

Die Anwenderinnen und Anwender müssen die Möglichkeit haben, persönliche Einstellungen wie Favoriten und Browsereinstellungen (z.B. Zoomstufe) so speichern zu können, dass diese auch nach Beenden und erneutem Start der Lösung zur Verfügung stehen.
Die persönlichen Einstellungen sind im Rahmen von Updates/Upgrades der gekapselten Webbrowser-Lösung zu erhalten, sodass für die Anwenderinnen und Anwender keine Einschränkungen entstehen.

Die Größe von Aktualisierungen ist möglichst klein zu halten, um Ressourcen (Übertragungsrate im Netzwerk, Datenvolumen) zu schonen und den Zeitbedarf entsprechend zu verkürzen (falls mögl. inkrementelle Updates).
Updates/Upgrades darf der Anbieter der gekapselten Webbrowser-Lösung auf einer Plattform seiner Wahl veröffentlichen. Es sollte die Möglichkeit geben, Updates/Upgrades von der Plattform herunterzuladen und anschließend in die zentrale Verwaltung importieren zu können. Die Verteilung zu den einzelnen Clients sollte von der zentralen Instanz aus der Infrastruktur des Auftraggebers möglich sein. Die automatisierte Prüfung der Integrität und Authentizität der Updates/Upgrades muss durch den Hersteller sichergestellt und nachprüfbar z.B. anhand des Hashwert

3.1.16 Virenscanner und andere Schutzfunktionen

Eine Funktion, die aktiv innerhalb der gekapselten Umgebung Inhalte des Internets auf bekannte Schadcode-Strukturen (z. B. Viren) analysiert, sollte vorhanden sein. Diese muss bei Erkennung schadhafter Inhalte die Anwenderin oder den Anwender warnen sowie entsprechend protokollieren. In Anbetracht einer Schnittstelle zum Client zur Übertragung heruntergeladener Inhalte ist eine derartige Funktion erforderlich (siehe 3.1.12).

3.1.17 Selbstschutz

Der Selbstschutz soll die eigene Software vor Manipulation auf dem System schützen, sodass die Software nicht geändert oder deaktiviert und dazugehörige Moduldateien verändert werden können.
(Ähnlich wie bei McAfee)

4 TECHNISCHE ANFORDERUNGEN AN DAS TOOL

Im folgenden Kapitel werden die technischen Anforderungen an die zu implementierende Lösung definiert.

4.1 Systemplattform & Technologiebasis

4.1.1 Plattform Kompatibilität Windows 10 & Windows 11

Die Lösung muss mit Microsoft Windows 10 (64bit), Microsoft und Windows 11 (64bit) kompatibel sein. Eine Unterstützung für 32bit wäre wünschenswert ist aber kein muss.
In verschiedenen Bereichen, z. B. der Telearbeit, werden VPN eingesetzt. Die gekapselte Webbrowser-Lösung muss mit dem in der Landesverwaltung üblichen VPN-Verfahren (derzeit NCP) einsetzbar sein. Ein Betrieb der Lösung über schmalbandige Verbindungen (mindestens 4Mbit/s) muss ohne wesentliche Einbuße möglich sein.

4.1.2 Kompatibilität mit 2 Proxy Lösung

Die Behörden des Landes NRW greifen auf Webseiten im Internet bzw. im Intranet über eine 2 Proxy-Lösung zu.

4.1.3 Mandantenfähigkeit (Zentrale Verwaltung Rollen- und Rechtekonzept der Administration)

Die Lösung sollte Mandantenfähig sein, dabei sollen die jeweils definierten Policies und Einstellung untereinander getrennt sein. Die Administration der Mandanten muss auch hier voneinander getrennt sein. Hierbei ist auch das Rollen- und Rechtekonzept der Administration zu beachten. (siehe 3.1.8)

4.1.4 BSI Mindeststandard Anforderung des BSI Web Browser (Sandboxing und Kapselung)

- Der Web-Browser MUSS eine Architektur mit folgenden Eigenschaften bereitstellen: Sämtliche Komponenten MÜSSEN voneinander und zum Betriebssystem hin gekapselt sein. Darstellungskomponenten für aktive Inhalte wie Flash und JavaScript MÜSSEN vom Hauptprozess gekapselt sein.
-

4.1.5	Webseiten MÜSSEN voneinander isoliert werden. Die Isolierung SOLLTE in Form eigenständiger Prozesse erfolgen. Eine Isolation auf Thread-Ebene ist aber auch zulässig.BSI Ransomware Maßnahme Katalog	

Die vom BSI angeforderten Maßnahmen zum Thema Ransomware müssen eingehalten werden.

4.2 Security & Datensicherheit

A-1. Keine Kommunikation zu Dritten

Das System sollte die Sicherheit und Vertraulichkeit der darin abgelegten Daten sicherstellen. Insbesondere darf das Produkt keine Funktionalitäten zum Ausspähen von Daten enthalten, keine Informationen über IT-Systeme, deren Daten, oder das Benutzerverhalten an Dritte übermitteln, oder derart speichern, dass Dritte darauf Zugriff nehmen könnten.

A-2. Einsatz aktueller Technologien

Der Hersteller der angebotenen Lösung muss sicherstellen, dass er nur Technologien von Drittanbietern verwendet, die von dem jeweiligen Hersteller auch noch aktiv gewartet/supportet werden. Sofern der Support einer verwendeten Technologie während der Vertragslaufzeit (4 Jahre) eingestellt wird, müssen diese spätestens zum offiziellen Supportende vollständig ersetzt werden.

A-3. Information zur sicherheitsrelevanten Risiken in den verwendeten Technologien

Der Anbieter muss über Sicherheitslücken in den von ihm verwendeten und implementierten Technologien aktiv informieren.