

# **IT-Rahmenbedingungen im Landesbetrieb Straßenbau Nordrhein- Westfalen**

**Version: 1.4**

**Datum: 03.11.2025**

Bei der Ausschreibung oder Entwicklung von Software sind die in den folgenden Abschnitten aufgeführten IT-Rahmenbedingungen zu beachten.

Abweichungen von diesen Vorgaben sind im Vorfeld abzustimmen und ausführlich zu begründen sowie der Nutzen für den Landesbetrieb darzulegen. Straßen.NRW entscheidet darüber, ob abweichende Lösungen zum Einsatz kommen können.

Grundsätzlich wird besonders hoher Wert auf eine stabile Softwarearchitektur mit minimalem Installations-, Konfigurations- und Wartungsaufwand gelegt. Im Landesbetrieb ist parallel zum Produktivsystem eine Qualitätssicherungsumgebung einzurichten.

Verträge im IT-Bereich werden regelmäßig auf Basis der Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT), herausgegeben vom Beauftragten der Bundesregierung für Informationstechnik (kurz CIO Bund), geschlossen. Straßen.NRW entscheidet darüber, ob abweichende Lösungen zum Einsatz kommen können.

**Die stetige Aufrechterhaltung und Verbesserung der Informationssicherheit richtet sich nach dem IT-Grundschutzkompendium des Bundesamtes für Sicherheit in der Informationstechnik.**

## Inhalt:

|       |                                               |   |
|-------|-----------------------------------------------|---|
| 1     | Netzwerk .....                                | 3 |
| 1.1   | Netzwerkzugriff .....                         | 3 |
| 1.2   | Bandbreite .....                              | 3 |
| 2     | Server .....                                  | 4 |
| 2.1   | Serverbetriebssystem .....                    | 4 |
| 2.2   | Weitere Server-Komponenten .....              | 4 |
| 2.3   | Datenbanken .....                             | 4 |
| 3     | Client .....                                  | 5 |
| 3.1   | Betriebssystem und Office Lösung .....        | 5 |
| 3.2   | Software .....                                | 5 |
| 3.3   | Softwareinstallation .....                    | 5 |
| 3.4   | Softwarebetrieb .....                         | 5 |
| 3.4.1 | Lizensierung von Software .....               | 6 |
| 3.4.2 | Bestandteile der Software .....               | 6 |
| 3.4.1 | Freiheit von Schadsoftware und „no spy“ ..... | 7 |
| 4     | Mobilgeräte .....                             | 7 |
| 4.1   | Mobile Betriebssysteme .....                  | 7 |
| 4.2   | Verteilung/ Berechtigungen von Apps .....     | 8 |
| 5     | Webanwendungen .....                          | 8 |
| 6     | Anschlüsse externer Geräte .....              | 9 |
| 6.1   | Raumausstattung .....                         | 9 |
| 7     | Cloudnutzung .....                            | 9 |
| 8     | KI-Nutzung .....                              | 9 |

# 1 Netzwerk

## 1.1 Netzwerkzugriff

Der Landesbetrieb Straßenbau NRW betreibt ein eigenes, an das Landesverwaltungsnetz NRW angeschlossenes Weitverkehrsnetz. Der Zugang zum Landesverwaltungsnetz wird mit Hilfe einer Firewall abgesichert.

Der Zugriff aus dem eigenen Weitverkehrsnetz über das Landesverwaltungsnetz auf Ressourcen im Internet ist stark reglementiert. Ausgehende Verbindungen dürfen nur durch wenige Protokolle aufgebaut werden. **Der Aufbau von Verbindungen aus dem Internet in das Landesverwaltungsnetz ist nicht gestattet.**

Für administrative Fernzugriffe aus dem Internet wird eine durch den zentralen IT-Dienstleister des Landes zur Verfügung gestellte Software, Fastviewer, eingesetzt. **Alternative Produkte sind nicht zulässig.**

## 1.2 Bandbreite

Die Leitungsbandbreite für verteilte Installationen beträgt minimal 10 Mbit/s. Fast alle Standorte verfügen über eine bessere Anbindung (Meistereien i.d.R. 100 Mbit/s, Niederlassungen 1000 Mbit/s). Die verfügbaren Bandbreiten richten sich somit nach dem Einsatzort und den Verbindungen der Software. Maßgeblich ist immer die minimale Bandbreite in einem auch zukunftsicheren Einsatzszenario.

Hierbei ist zudem zu berücksichtigen, dass die angegebene Bandbreite nicht ausschließlich für das geplante Produktsystem zur Verfügung steht, sondern für alle Einsatzzwecke wie z.B. VOiP. Ebenfalls ist damit zu rechnen, dass die vorhandenen Leitungskapazitäten zukünftig durch weitere, zusätzliche Anwendungen belastet werden können.

## 2 Server

### 2.1 Serverbetriebssystem

Als Serverbetriebssystem kommt im Bestand Microsoft Windows Server 2019 zum Einsatz. Neuinstallationen werden mit Windows Server 2022 durchgeführt.

In wenigen, begründeten Einzelfällen kommt auch Suse Linux Enterprise zum Einsatz.

Im Standardfall werden zentrale Fachanwendungen auf virtuellen Serversystemen betrieben. Neuentwicklungen müssen hierfür ausgelegt sein. Die virtuellen Serversysteme basieren auf VMware Infrastructure 7.0.3. Hier ist eine Aktualisierung geplant, von daher ist die Voraussetzung 7.0.3 oder höher.

### 2.2 Weitere Server-Komponenten

Es wird das Microsoft Active Directory verwendet. Wenn eine Benutzer- oder Rechteverwaltung vorgesehen ist, muss diese über das Active Directory mittels LDAPS inklusive SSO realisiert sein.

Zum Schutz vor Computerviren und sonstiger, schadender Software wird flächendeckend eine Antivirus-Software in der aktuellen Version sowohl auf den Servern als auch auf den Clients eingesetzt.

Häufig wird auch eine Veröffentlichung per Citrix genutzt. Die zu entwickelnde oder zu beschaffende Anwendung sollte deshalb unter Citrix lauffähig sein. Ist dies nicht der Fall ist dies mit Straßen.NRW abzustimmen. In unserer Citrix Umgebung wird aktuell die Version Citrix XenApp 2203 eingesetzt. Diese ist bei der Entwicklung mindestens zugrunde zu legen, wobei eine Aktualisierung geplant ist. Von daher ist die Voraussetzung 2203 oder höher.

Als Webserver werden Microsoft IIS und Apache Tomcat unterstützt.

### 2.3 Datenbanken

Das Standard-Datenbankmanagementsystem ist MS SQL Server 2019. Auch dies ist als Mindestvoraussetzung anzusehen, höhere Versionen sind zulässig.

In zu begründenden und zu genehmigenden Ausnahmefällen können auch PostgreSQL Datenbanken (gegebenenfalls mit PostGIS-Erweiterung) eingesetzt werden.

Sollte die Anforderung nach anderen Datenbanksystemen bestehen, sind diese vorab mit der IT des Auftraggebers abzustimmen.

## 3 Client

### 3.1 Betriebssystem und Office Lösung

Als Betriebssystem auf den Clients wird Windows 11 Enterprise in 64-bit in einer der jeweils vom Hersteller aktuell unterstützten Version eingesetzt.

Als Office-Lösung kommt Microsoft Office 2021 Professional Plus in 64-bit zum Einsatz. Neu zu entwickelnde Software muss jedoch uneingeschränkt mit allen von Microsoft unterstützten Office-Versionen kompatibel sein.

Als Standardinternetbrowser ist nur Microsoft Edge in einer der jeweils vom Hersteller aktuell unterstützten Version freigegeben. Die Installation von Edge-Add-Ons ist unterbunden.

Der Zugriff auf den Microsoft Store wird ebenfalls unterbunden.

Insgesamt werden im Netz des Landesbetriebes etwa 3.650 Clients betrieben.

### 3.2 Software

### 3.3 Softwareinstallation

Installationen und Software-Updates erfolgen mittels automatisierter Verteilung der Anwendungen über das System Empirum der Firma Matrix42.

Die zu entwickelnde Anwendung muss hierfür zwingend über einen paketierbaren Installer, am besten im MSI-Format, verfügen und sich über entsprechenden Parameter silent, also ohne Benutzerinteraktion, automatisch installieren lassen.

**Anwendungen haben grundsätzlich keine Möglichkeit, eine Internetverbindung aufzubauen**, insbesondere auch im Rahmen der Installation! Dies ist beim Design der zu entwickelnden Anwendung bzw. dem Angebot zu berücksichtigen.

### 3.4 Softwarebetrieb

Regelmäßige, die IT-Sicherheit und ggf. fachliche Belange betreffende Updates müssen bereitgestellt werden. Insbesondere bei Sicherheitslücken in der Anwendung sind schnellstmögliche Patches erforderlich.

**Noch mal der Hinweis: Anwendungen haben grundsätzlich keine Möglichkeit, eine Internetverbindung aufzubauen.** Dies ist beim Design der zu entwickelnden Anwendung bzw. dem Angebot auch im Hinblick auf das Lizenzmanagement zu berücksichtigen!

### 3.4.1 Lizenzierung von Software

Software kann auf unterschiedlichem Wege lizenziert werden. Die Art der Lizenzierung ist detailliert darzustellen.

Wenn für den Einsatz der Software eine Netzwerklizenzierung vorgesehen ist wird die Bereitstellung über einen on-premises-Lizenzserver bevorzugt oder einem vergleichbaren System.

Alternative Lizenzierungsmechanismen, wie z. B. Cloudlizenzserver, müssen mit einer durch Proxy abgesicherten Netzwerkumgebung kompatibel sein. Eine direkte Kommunikation der Clients ins Internet ist aus Sicherheitsgründen nur sehr eingeschränkt möglich. Erforderliche Proxykonfigurationen müssen unterstützt, automatisiert einstellbar und dokumentiert sein. Des Weiteren sollte die Möglichkeit bestehen, Test- und Schulungslizenzen zu erhalten. Diese sollen für definierte Zeiträume mit vollem oder eingeschränktem Funktionsumfang zur Verfügung stehen, um interne Schulungen und Test- und Pilotprojekte durchführen zu können.

### 3.4.2 Bestandteile der Software

Die angebotene Software darf ausschließlich solche Komponenten enthalten, die für den Betrieb und die Funktionalität der Anwendung zwingend erforderlich sind. Es dürfen keine nicht notwendigen oder versteckten Module, Bibliotheken oder Dienste integriert sein, die Daten ohne ausdrückliche Zustimmung des Auftraggebers an externe Server oder Dritte übertragen (z. B. Telemetrie, Tracking, „Schnüffelsoftware“). Der Anbieter garantiert, dass sämtliche eingesetzte Softwarebestandteile datenschutzkonform sind und keine unerlaubte Datenübermittlung erfolgt. Eventuelle Telemetrie- oder Diagnosefunktionen müssen transparent offengelegt und nur mit Einwilligung aktiviert werden.

In der Software enthaltene Third-Party Produkte sind vollständig aufzuführen und der Einsatzzweck dazulegen. Es muss sichergestellt sein, dass diese regelmäßigen Updates erfahren!

Insbesondere im Fall von möglichen, kritischen Sicherheitslücken muss schnellstmöglich ein entsprechender Patch der gesamten Anwendung zur Verfügung gestellt werden.

Weiterhin sind häufig gemeinsam genutzte Komponenten, wie Lizenztools, jeweils auf dem aktuellen Stand zu halten, um eine Lauffähigkeit im gemeinsamen Verbund sicher zu stellen.

Hierzu ist Straßen.NRW eine Software Bill of Material (SBOM) zur Verfügung zu stellen, die während des vertraglich vereinbarten Dienstleistungszeitraumes stets zu aktualisieren ist. Die SBOM soll einen detaillierten Überblick über die verwendeten Programmbibliotheken und Komponenten der Software geben. Somit kann Straßen.NRW zu jedem Zeitpunkt nachvollziehen, welche Bestandteile in die Software geflossen sind, um zukünftig mögliche Sicherheitslücken zu schließen. Folgende Datenfelder sollten in der SBOM mindestens enthalten sein:

- Name des Anbieters einer Komponente
- Komponentename (ursprüngliche Bezeichnung des Entwicklers)

- Version der Komponente
- eindeutige Identifikatoren (Nachschlüssel)
- Zeitstempel von der Zusammenstellung der SBOM-Daten
- Autor der SBOM-Daten

### 3.4.1 Freiheit von Schadsoftware und „no spy“

Analog zur Ziffer 2.3 der EVB-IT Überlassung AGB darf die Software keine Schadkomponenten oder Bestandteile zur Datenausleitung/ -sammlung besitzen, die nicht im Sinne des Auftraggebers sind. Konkreter der Wortlaut der AGB:

*„ Der Auftragnehmer überlässt die Standardsoftware „ frei von Schaden stiftender Software“. Dies ist mit aktueller Scan-Software zu einem angemessenen Zeitpunkt vor der Lieferung zu prüfen. Der Auftragnehmer erklärt, dass die Prüfung keinen Hinweis auf Schaden stiftende Software\* ergeben hat. Diese Regelung gilt für jede, auch die vorläufige und Vorabüberlassung, z.B. zu Testzwecken.*

*Der Auftragnehmer gewährleistet darüber hinaus, dass die von ihm zu liefernde Standardsoftware\* frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der Standardsoftware\*, anderer Soft- und/oder Hardware oder von Daten gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen durch*

- *Funktionen zum unerwünschten Absetzen/Ausleiten von Daten,*
- *Funktionen zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik oder*
- *Funktionen zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen.*

*Unerwünscht ist eine mögliche Aktivität einer Funktion, wenn die Aktivität so weder vom Auftraggeber in seiner Leistungsbeschreibung gefordert, noch vom Auftragnehmer unter konkreter Beschreibung der Aktivität und ihrer Funktionsweise angeboten, noch im Einzelfall vom Auftraggeber ausdrücklich autorisiert („opt-in“) wurde.“*

## 4 Mobilgeräte

Den Mitarbeitenden können dienstlich bereitgestellte Smartphones zur Verfügung gestellt werden. Die Ausstattung erfolgt nicht flächendeckend, sondern bedarfsgerecht. Daher darf nicht davon ausgegangen werden, dass die Zielgruppe Ihrer IT-Lösung in jedem Fall über ein Smartphone verfügt. Dies ist vorab mit der IT des Auftraggebers zu besprechen.

### 4.1 Mobile Betriebssysteme

Zum Einsatz kommen neben Apple iPhone auch verschiedene Geräte der Marke Samsung.

Android und iOS werden in den jeweils aktuellen Versionen sowie übergangsweise in der vorherigen Version eingesetzt.

## **4.2 Verteilung/ Berechtigungen von Apps**

Alle Mobilgeräte werden per Mobile Devicemanagement verwaltet. Darüber können Apps obligatorisch oder optional auf den Mobilgeräten zur Verfügung gestellt werden. Zu beachten ist, dass die Unternehmensumgebung in einem gesicherten Container betrieben wird. Apps können daher nicht auf E-Mails, Kalender oder Kontakte aus dem Unternehmensbereich zugreifen.

Sollte eine Anforderung dahingehend bestehen, ist dies vorab mit der IT des Auftraggebers abzustimmen.

## **5 Webanwendungen**

Bei Webanwendungen gibt es keine vorgegebenen Programmier- und/oder Skriptsprachen, Frameworks, Bibliotheken (Java) oder sonstigen Packages (JavaScript). Ebenso keine Vorgaben hinsichtlich eines Compilers bzw. einer Laufzeitumgebung wie z.B. Java Virtual Machine oder .NET Common-Language-Runtime.

Die Umsetzung muss sich an zum Zeitpunkt der Umsetzung aktuellen und absehbaren Entwicklungen orientieren und VORAB als Konzept oder Beschreibung von der IT-Abteilung genehmigt werden.

## 6 Anschlüsse externer Geräte

Hierunter fallen Geräte, die z.B. zur Raumausstattung gehören wie Beamer oder Fernseher, Messgeräte für technische Zwecke oder ähnliches.

### 6.1 Raumausstattung

Für Geräte zur Bildwiedergabe sind zwei Anschlusswege vorgesehen. Einmal kabelgebunden über den weit verbreiteten Standard HDMI und ohne Kabel mit dem System ClickShare der Firma Barco.

## 7 Cloudnutzung

Es gibt in der Landesverwaltung von Nordrhein-Westfalen noch keine veröffentlichte Richtlinie für die Nutzung von Cloudverfahren.

Es sind jedoch folgende Punkte zu beachten, unabhängig von der Art der Cloudnutzung wie z.B. als reiner Ablageort und als Erweiterung der eigenen Infrastruktur (IaaS), als einzelne Softwarelösung (SaaS) oder als komplettes System (PaaS):

- Cloudstandort vorzugsweise in der Bundesrepublik Deutschland, jedoch nicht außerhalb des europäischen Wirtschaftsraumes.
- Die Kriterien des Kriterienkatalogs Cloud Computing C5 des BSI sollten vom Anbieter eingehalten werden, Abweichungen sind im Einzelfall vorab zu prüfen.
- Als Vertragsgrundlage dient der EVB-IT-Cloudvertrag, Abweichungen hiervon sind im Einzelfall vorab zu prüfen.

## 8 KI-Nutzung

Die Nutzung von KI unterliegt engen Grenzen, es gibt noch keine verbindliche Richtlinie des Landes NRW, gleichwohl eine von Straßen.NRW. Die Verarbeitung und Speicherung von dienstlichen Daten und insbesondere personenbezogenen Daten unterliegen aktuell strengen Regeln.

Der Ort der Datenspeicherung die Art der Verarbeitung sind für den Anwendungsfall darzulegen.