



Planung

Leistungsbeschreibung Videowand

Version 1.0

Stand: 16.09.2026

Klassifizierung

Geheimchutz: ☐ VS-NfD

Verteiler: ☐ BDBOS ☐ AS

Inhaltsverzeichnis

Begriffsdefinitionen	3
1 Leistungsbeschreibung	5
2 Zielsetzung und Projektgegenstand	5
3 Zielbild der Systemarchitektur	5
4 Netz- und Sicherheitsarchitektur	6
5 Informationssicherheit, Systemhärtung und Fernwartung	7
6 Funktionale und technische Anforderungen	7
6.1 Visualisierung und Layoutmanagement	7
6.2 Quellen- und Datenintegration	8
6.3 Bedienung und Administration	9
6.4 Automatisierung und ereignisbasierte Darstellung	9
7 Anforderungen an Verfügbarkeit und Betrieb	10
8 Monitoring, Protokollierung und Auditfähigkeit	10
9 Notfallbetrieb, Fallback und Störungsklassen	11
10 Hardwareanforderungen	11
10.1 LED Videowand	12
10.2 Monitore	12
11 Testumgebung	12
12 Beistellungspflichten der Auftraggeberin	13
13 Installation und Inbetriebnahme	13
14 Dokumentation und Schulung	13
15 Abnahme	14
16 Betrieb und Support	14
17 Zusammenfassung der MUSS Anforderungen	15
Anhang 19	

Begriffsdefinitionen

Für diese Leistungsbeschreibung gelten die nachfolgenden Begriffsdefinitionen. Sie dienen der einheitlichen Auslegung der Anforderungen und sind bei Angebotserstellung, Umsetzung, Dokumentation und Abnahme zugrunde zu legen.

Begriff	Definition
Lösung	Gesamtheit aller durch die Auftragnehmerin zu liefernden, zu integrierenden und betriebsfertig zu übergebenden Komponenten, Systeme, Softwarebestandteile, Steuerungsfunktionen, Dienstleistungen, Dokumentationen und Schulungen.
Videowand	Die physische Anzeigefläche beziehungsweise Anzeigeeinheit, auf der Inhalte großflächig dargestellt werden. Die Videowand ist als logisch zusammenhängende Gesamtfläche zu betreiben.
Videowandsystem	Technisches Gesamtsystem zur Steuerung, Verwaltung, Verarbeitung und Darstellung von Inhalten auf der Videowand, einschließlich Controller-, Management-, Zuspil-, Netzwerk- und Softwarekomponenten.
Quelle	Ein eigenständiges Ausgangssignal, eine virtuelle Sitzung, ein Stream, ein Browserfenster, eine Anwendung, ein Dashboard, ein Fachverfahren oder eine sonstige darstellbare Informationsquelle.
Sicherheitsdomäne	Ein logisch oder physisch abgegrenzter Netz- beziehungsweise Schutzbereich mit eigenen Sicherheitsanforderungen, Zugriffsregeln und Kommunikationsgrenzen. In der Regel mit strikter Trennung vom Internet.
Layoutprofil	Gespeicherte Anordnung von Quellen, Darstellungsflächen, Fenstern, Größen, Positionen und gegebenenfalls ereignisabhängigen Anzeigeelementen auf der Videowand.
SIEM	Security Information and Event Management; zentrales System zur Sammlung, Korrelation, Analyse und Alarmierung sicherheitsrelevanter Ereignisse und Protokolldaten aus unterschiedlichen IT-Systemen. Ein SIEM unterstützt die Erkennung von Sicherheitsvorfällen, die Nachvollziehbarkeit von Systemereignissen sowie die revisionsfähige Auswertung sicherheitsrelevanter Aktivitäten.

Mandantenfähigkeit / Mandat	Mandantenfähigkeit bezeichnet die Fähigkeit der Lösung, mehrere organisatorisch, fachlich oder sicherheitsbezogen getrennte Nutzergruppen beziehungsweise Einsatzbereiche innerhalb einer gemeinsamen Plattform logisch voneinander abzugrenzen. Ein Mandat ist dabei ein eindeutig abgegrenzter Verwaltungs-, Berechtigungs- oder Nutzungskontext, dem Benutzer, Rollen, Quellen, Layouts und Inhalte zugeordnet werden können.
Newsticker	Systemfunktion zur manuellen und optional automatisierten Anzeige kurzer Informations- oder Lagehinweise innerhalb definierter Layouts.
Auftraggeberin	Die ausschreibende Stelle beziehungsweise spätere Betreiberin der Lösung.
Auftragnehmerin	Das beauftragte Unternehmen, das die ausgeschriebenen Leistungen erbringt und die Lösung betriebsfertig übergibt.
BOS	Behörden und Organisationen mit Sicherheitsaufgaben

1 Leistungsbeschreibung

Das Dokument handelt von der Integration und dem Betrieb einer zentralen Videowand- und Visualisierungsplattform für Leitstellen- und Lagezentren in der ALDB GmbH.

2 Zielsetzung und Projektgegenstand

Gegenstand der Leistung ist die Lieferung, Implementierung, Integration, Inbetriebnahme und betriebsfertige Übergabe einer zentral administrierbaren Videowand- und Visualisierungsplattform für den Einsatz in Leitstellen-, Lage- und Kollaborationsumgebungen.

Die zu beschaffende Lösung hat die bestehende, technisch fragmentierte Multi-Monitor- und Einzelarbeitsplatzstruktur abzulösen und eine logisch zusammenhängende, zentral steuerbare Visualisierungsumgebung bereitzustellen. Ziel ist die Schaffung einer zentralen Lage- und Informationsplattform, auf der Inhalte aus unterschiedlichen Fachverfahren, Netzsegmenten und Datenquellen gleichzeitig, lageabhängig und dynamisch dargestellt werden können.

Die Videowand ist nicht als Erweiterung einzelner Arbeitsplatzmonitore, sondern als eigenständiges, zentral verwaltetes Visualisierungssystem für Leitstellen- und Lagebetriebsprozesse auszulegen.

Die angebotene Lösung muss insbesondere die nachfolgenden Mindestanforderungen erfüllen:

- hochverfügbarer und wartungsfreundlicher Betrieb,
- modulare Erweiterbarkeit zum Kapazitätsausbau,
- netztechnisch sichere Trennung von Sicherheitsdomänen,
- zentrale Administration und Steuerung,
- Eignung für den 24/7-Dauerbetrieb in einsatzkritischen Umgebungen.

Zum Leistungsumfang gehören die technische Plattform sowie sämtliche hierfür erforderlichen Integrations-, Management-, Steuerungs-, Dokumentations-, Schulungs- und Betriebsleistungen, soweit sie für eine betriebsfertige Übergabe erforderlich sind.

3 Zielbild der Systemarchitektur

Angestrebt wird eine moderne, zentral administrierbare und netzwerkfähige Videowandarchitektur mit flexiblem Quellenmanagement und zentraler Steuerung.

Die Architektur soll insbesondere folgende Eigenschaften aufweisen:

- logische Gesamtfläche der Videowand unabhängig von physischer Monitorstruktur,
- dynamische Segmentierung und freie Inhaltsplatzierung,
- parallele Darstellung mehrerer Quellen unterschiedlicher Herkunft,
- Unterstützung browserbasierter Anwendungen und dashboardbasierter Visualisierungen

- zentrale Layout-, Szenen- und Benutzerverwaltung,
- Integration physischer und virtueller Quellen,
- Integration bestehender Fachverfahren,
- hohe Skalierbarkeit,
- sowie mandantenfähige und rollenbasierte Bedienkonzepte.

Die Verarbeitung, Steuerung und Verteilung von Bildsignalen muss über eine zentral administrierbare, skalierbare und netzwerkfähige Architektur erfolgen. IP-basierte, softwaredefinierte oder KVM-basierte Lösungsansätze sind zulässig, sofern sie die Anforderungen an flexible Quellenverwaltung, sichere Netztrennung, zentrale Bedienung und Erweiterbarkeit erfüllen. Starre, nicht zentral administrierbare Punkt-zu-Punkt- oder HDMI-Matrixarchitekturen sind zu vermeiden.

Die Lösung soll insbesondere moderne Betriebsmodelle unterstützen, bei denen:

- mehrere Webanwendungen,
- Dashboards,
- GIS-Systeme,
- Videokonferenzsysteme,
- Kamera- und VMS-Systeme,
- sowie Echtzeitdatenquellen parallel und dynamisch auf der Videowand dargestellt werden können.

Dabei ist zu berücksichtigen, dass zukünftige Visualisierungen zunehmend webbasiert, virtualisiert oder zentral bereitgestellt erfolgen und nicht zwingend an dedizierte physische Zuspil-PCs gekoppelt sein müssen

4 Netz- und Sicherheitsarchitektur

Ein besonderer Schwerpunkt der Beschaffung liegt auf der sicheren Verarbeitung und Darstellung von Informationen aus unterschiedlichen Sicherheitsdomänen.

Die Lösung muss den parallelen Betrieb mindestens folgender Netzbereiche unterstützen:

Zwischen den Netzsegmenten darf keine unzulässige Kommunikation entstehen. Die Netztrennung darf weder durch die Videowandplattform noch durch Management-, Steuerungs- oder Visualisierungskomponenten aufgehoben oder umgangen werden.

Insbesondere gilt:

- keine gemeinsame Verarbeitung unterschiedlicher Sicherheitsdomänen auf einem gemeinsamen Betriebssystem oder Client,
- keine Routing-, Bridging- oder Proxyfunktion zwischen Netzbereichen,
- Unterstützung physisch getrennter Air-Gap-Architekturen,
- vollständiger On-Premise-Betrieb aller zentralen Komponenten,
- keine Cloud-Abhängigkeit,
- keine aktiven Funktechnologien oder hardwareseitig deaktivierbare Funkmodule.

Die parallele Darstellung von Informationen aus unterschiedlichen Sicherheitsdomänen auf derselben Videowand muss möglich sein, ohne dass hierdurch die geforderte Trennung der Netz- und Sicherheitsbereiche beeinträchtigt wird.

5 Informationssicherheit, Systemhärtung und Fernwartung

Die angebotene Lösung muss für den Einsatz in einem sicherheitskritischen BOS-nahen Betriebsumfeld geeignet sein. Alle zentralen Komponenten, Managementsysteme, Betriebssysteme, Dienste und Schnittstellen sind nach anerkannten Grundsätzen der IT-Sicherheit zu härten. Nicht benötigte Dienste, Ports, Protokolle, Benutzerkonten, Funktechnologien und Schnittstellen sind zu deaktivieren oder technisch zu unterbinden.

Fernwartung darf nur nach vorheriger Freigabe durch die Auftraggeberin erfolgen. Ein permanenter externer Zugriff auf die Lösung ist nicht zulässig. Fernwartungszugänge müssen deaktivierbar, zeitlich begrenzbare, eindeutig authentisierbar und vollständig protokollierbar sein. Cloud-Relay-Dienste, herstellereigene Fernzugriffsplattformen oder sonstige externe Vermittlungsdienste dürfen nur eingesetzt werden, wenn diese durch die Auftraggeberin ausdrücklich freigegeben wurden.

Die Auftragnehmerin hat offenzulegen, ob und in welchem Umfang Hersteller, Unterauftragnehmer oder Supporteinheiten Zugriff auf Systemkomponenten, Protokolldaten, Konfigurationen oder dargestellte Inhalte erhalten können.

6 Funktionale und technische Anforderungen

6.1 Visualisierung und Layoutmanagement

Die Videowand muss als logisch zusammenhängende Gesamtfläche betrieben werden können. Inhalte müssen unabhängig von der physischen Monitorstruktur frei positionierbar, skalierbar, über mehrere Displays hinweg darstellbar und in vordefinierten Bereichen angeordnet werden können.

Das System muss eine flexible Segmentierung der Gesamtfläche in mehrere Darstellungsbereiche sowie die Darstellung von Quellen als Bild-in-Bild, Kachelansicht oder frei platzierbare Fenster unterstützen.

Das System muss je Videowand mindestens zehn voneinander unabhängige Quellen gleichzeitig darstellen können. Als Quelle gilt jeweils ein eigenständiges Ausgangssignal beziehungsweise eine eigenständige virtuelle Sitzung. Die gleichzeitige Darstellung weiterer Quellen muss durch Austausch, Umschaltung oder Erweiterung der dargestellten Quellen möglich sein; technische Begrenzungen je Videowand sind im Angebot transparent zu benennen.

Layoutprofile, Szenen und lagebezogene Darstellungszustände müssen gespeichert, versioniert, benutzer- oder rollenbezogen bereitgestellt und im laufenden Betrieb ohne Neustart aufgerufen werden können. Das Anlegen, Ändern, Freigeben und Aufrufen dieser Profile ist über das Rollen- und Rechtekonzept zu steuern und muss auch für den Nutzer ohne Admin Unterstützung möglich sein

Nach einem technischen Neustart oder Wiederanlauf muss das zuletzt aktive Layout automatisch wiederhergestellt werden können, sofern dem keine sicherheits- oder betriebsbedingten Einschränkungen entgegenstehen.

Die Beschaffung umfasst aktuell ein Videowandsystem an einem Standort. Die Lösung soll jedoch so ausgelegt sein, dass eine spätere Erweiterung um weitere Standorte beziehungsweise ein zweites Videowandsystem grundsätzlich möglich ist. Hierfür erforderliche Netzwerk-, Lizenz-, Sicherheits- oder Systemvoraussetzungen sind im Angebot als perspektivische Erweiterungsoption gesondert darzustellen.

Die Lösung muss lageabhängige Umschaltungen sowie zukünftige Automatisierungs- und Szenariosteuerungen unterstützen. Sofern hierfür zusätzliche Komponenten oder Lizenzen erforderlich sind, sind diese gesondert zu benennen.

6.2 Quellen- und Datenintegration

Die Plattform muss unterschiedliche physische, virtuelle und webbasierte Quellen parallel darstellen, zentral verwalten und eindeutig einer Sicherheitsdomäne beziehungsweise einem Netzsegment zuordnen können.

Hierzu zählen insbesondere:

- browserbasierte Fachverfahren,
- Web-Dashboards,
- Echtzeitdatenquellen,
- GIS-Anwendungen,
- Video- und Kamerasysteme,
- Videokonferenzlösungen,
- Audio-/Videoquellen,
- externe Präsentationssysteme,
- sowie temporäre mobile Zuspieldatenquellen.

Die Architektur soll bevorzugt virtuelle beziehungsweise softwaredefinierte Quellen unterstützen. Der Einsatz dedizierter physischer PCs je Einzelvisualisierung ist auf das erforderliche Maß zu begrenzen und im Angebot zu begründen.

Quellen aus der VS-NfD-Umgebung werden derzeit über einen Citrix-Client bereitgestellt. Aus dieser Umgebung kann über TightGate Pro auf Inhalte der nicht verschlüsselten Umgebung zugegriffen werden. Die angebotene Lösung muss dieses Betriebsmodell berücksichtigen, ohne die geforderte

Netz- und Sicherheitstrennung zu beeinträchtigen. Abweichende oder ergänzende Integrationsvorschläge sind technisch und sicherheitsfachlich zu begründen.

Die Lösung muss moderne Visualisierungskonzepte unterstützen, bei denen mehrere Webanwendungen, Browserfenster, Streams, Dashboards oder virtuelle Sitzungen parallel aus zentral verwalteten Systemen bereitgestellt werden können.

Im Anhang „Netzwerkarchitektur für Leitstellen- & Lagezentren“ ist ersichtlich, wie die Quellen heute aufgeschaltet sind und woher sie stammen.

6.3 Bedienung und Administration

Das System muss vollständig zentral administrierbar und bedienbar sein. Eine lokale Bedienung direkt an Zuspiegelgeräten, Displays oder einzelnen Hardwarekomponenten darf im Regelbetrieb nicht erforderlich sein. Administration, Bedienung, Layoutverwaltung, Benutzerverwaltung und Systemüberwachung müssen rollenbasiert geregelt werden können. Mehrere berechnete Benutzer müssen das System gleichzeitig bedienen können, ohne sich gegenseitig unkontrolliert zu beeinflussen.

Die Bedienoberfläche muss als webbasierte Anwendung oder vergleichbare zentrale Managementoberfläche bereitgestellt werden. Sie muss im vorgesehenen Betriebsnetz verfügbar sein und darf keine Cloud-Dienste voraussetzen. Mandantenfähigkeit beziehungsweise eine gruppenbezogene Sicht auf freigegebene Inhalte, Quellen und Layouts soll unterstützt werden.

Die Plattform muss es im initialen Ausbau mindestens vier berechtigten Arbeitsplätzen ermöglichen, den Inhalt ihres jeweiligen Monitors beziehungsweise ausgewählter Anwendungen kontrolliert auf die Videowand zu übertragen. Eine spätere Erweiterung um zusätzliche Arbeitsplätze muss ohne grundlegende Änderung der Systemarchitektur möglich sein. Die Übertragung darf ausschließlich innerhalb der jeweils zulässigen Sicherheitsdomäne erfolgen.

Die aktuell vorgesehenen Bedienplätze verfügen über bestehende Monitorarbeitsplätze mit insgesamt zwei HD- und zwei WQHD-Monitoren. Die angebotene Lösung muss diese Ausgangssituation berücksichtigen und eine kontrollierte Übertragung der jeweiligen Monitorinhalte beziehungsweise ausgewählter Anwendungen auf die Videowand ermöglichen.

6.4 Automatisierung und ereignisbasierte Darstellung

Das System muss als Bestandteil der Basislösung einen internen Newsticker bereitstellen. Dieser muss durch berechnete Personen manuell gepflegt, aktiviert, deaktiviert und in vordefinierten Layouts angezeigt werden können. Zusätzlich soll der Newsticker automatisierte Einspeisungen, beispielsweise aus definierten Nachrichten- oder Informationskanälen, unterstützen. Herkunft, Berechnungen, Anzeigzeitraum und Protokollierung der eingestellten Inhalte sind nachvollziehbar abzubilden.

Die Lösung muss ereignisbasierte Darstellungen unterstützen. Hierzu zählen insbesondere das automatische Aufrufen vordefinierter Layouts bei definierten Auslösern, die Verarbeitung potenzialfreier Kontakte sowie die Ansteuerung ergänzender Signalisierungen, etwa Hintergrundbeleuchtungen oder externe Signalleuchten. Unterstützte Schnittstellen und Automatisierungsregeln sind im Angebot zu beschreiben.

Ereignisse unterschiedlicher Kritikalität müssen visuell unterscheidbar dargestellt werden können, beispielsweise durch Pop-ups, farbliche Hervorhebungen, Rahmen, Prioritätsanzeigen oder vergleichbare Darstellungsformen. Die konkreten Kritikalitätsstufen und Auslösebedingungen sind im Rahmen der Auftragsklärung festzulegen.

7 Anforderungen an Verfügbarkeit und Betrieb

Die Lösung ist für den 24/7-Dauerbetrieb in Leitstellen- und Lageumgebungen auszulegen. Planung, Dimensionierung und Komponentenauswahl müssen so erfolgen, dass der Ausfall einzelner Teilkomponenten nicht zum vollständigen Verlust der Visualisierungsfähigkeit führt.

Die Anforderungen an Monitoring, Protokollierung und Auditfähigkeit sind in Kapitel 10 konkretisiert.

Backup-, Wiederanlauf- und Wiederherstellungsmechanismen müssen durch die Auftragnehmerin bereitgestellt, dokumentiert und so ausgelegt werden, dass sie durch die Auftraggeberin eigenständig durchgeführt oder nachvollziehbar beauftragt werden können.

Eine vollständig redundante Gesamtauslegung wird nicht zwingend gefordert. Die Auftragnehmerin hat jedoch darzustellen, welche Redundanzoptionen für zentrale Komponenten, Netzteile, Steuerungsinstanzen, Zuspelwege und Managementfunktionen verfügbar sind und welche Auswirkungen diese auf Verfügbarkeit, Kosten, Platzbedarf und Betrieb haben.

Das System muss so aufgebaut sein, dass es ohne Umbau oder Austausch zentraler Komponenten hinsichtlich der Anzahl der Monitore und Mitarbeiterplätze modular erweiterbar ist.

8 Monitoring, Protokollierung und Auditfähigkeit

Die Lösung muss in ein bestehendes Betriebs- und Sicherheitsmonitoring integrierbar sein. Hierfür sind geeignete Schnittstellen, beispielsweise SNMP, Syslog, REST-API oder vergleichbare standardisierte Verfahren, bereitzustellen beziehungsweise zu beschreiben. Proprietäre Schnittstellen sind vollständig zu dokumentieren.

Mindestens folgende Zustände müssen überwacht oder zur Überwachung bereitgestellt werden können: Verfügbarkeit zentraler Komponenten, Status der Videowand und Einzelmonitore, Controller- und Serverstatus, Netzteil- und Lüfterzustand, Temperatur, Systemauslastung, Quellenverfügbarkeit, Lizenzstatus, Speicher- und Datenträgerzustand sowie Störungen an Schnittstellen oder Kommunikationswegen.

Die Lösung muss sicherheitsrelevante Ereignisse, insbesondere Benutzeranmeldungen, fehlgeschlagene Anmeldeversuche, Änderungen an Rollen und Rechten, Konfigurationsänderungen, Administratoraktionen sowie Fernwartungssitzungen, über geeignete Schnittstellen für die Übergabe an ein zentrales SIEM bereitstellen können. Unterstützte Protokolle, Datenformate, Filtermöglichkeiten, Zeitstempelung und Mechanismen zur Integritätssicherung der Protokolldaten sind im Angebot darzustellen.

Protokolldaten müssen exportierbar und für eine angemessene Prüf- und Nachweisführung auswertbar sein. Die Auftragnehmerin hat darzustellen, welche Aufbewahrungsfristen, Exportformate, Zeitquellen, Manipulationsschutzmechanismen und Schnittstellen zur zentralen Logauswertung unterstützt werden.

9 Notfallbetrieb, Fallback und Störungsklassen

Für den Betrieb in einer Leitstellen- und Lageumgebung ist ein Fallback- und Notfallbetriebskonzept vorzulegen. Dieses muss beschreiben, welche Mindestfunktionen bei Ausfall einzelner Komponenten, Managementsysteme, Zuspilwege, Netzwerkverbindungen oder Anzeigeflächen erhalten bleiben und wie der Regelbetrieb wiederhergestellt wird.

Das Konzept muss insbesondere eine definierte Mindestanzeige im Störfall, den Wiederanlauf des zuletzt aktiven Layouts, Ersatz- beziehungsweise Ausweichdarstellungen für wesentliche Quellen, den Umgang mit Teilausfällen sowie die Bedienbarkeit bei eingeschränktem Netz- oder Managementbetrieb beschreiben.

Störungen sind mindestens in die Klassen kritisch, hoch, mittel und niedrig zu unterteilen. Kritische Störungen liegen insbesondere vor, wenn die Videowand insgesamt nicht nutzbar ist oder der Lagebetrieb wesentlich beeinträchtigt wird. Hohe Störungen betreffen wesentliche Quellen, Layoutfunktionen oder zentrale Bedienfunktionen. Mittlere Störungen betreffen eingeschränkte Teilfunktionen; niedrige Störungen betreffen Fehler ohne unmittelbare Auswirkung auf den Lagebetrieb.

Für jede Störungsklasse sind Reaktionszeit, Wiederherstellungszeit, Eskalationsweg, Verfügbarkeit von Ersatzteilen, Remote- beziehungsweise Vor-Ort-Unterstützung sowie Herstellereskalation darzustellen. Sofern die angebotenen Serviceklassen von den geforderten Störungsklassen abweichen, ist die Zuordnung transparent zu erläutern.

10 Hardwareanforderungen

Die eingesetzte Hardware muss für den professionellen 24/7-Betrieb in einsatzkritischen Umgebungen geeignet sein. Alle netzwerkfähigen Komponenten müssen IPv4 und IPv6 unterstützen.

In welchen Räumlichkeiten die Komponenten verbaut werden sollen, ist dem Anhang „Ausstattung Berlin“ zu entnehmen.

10.1 LED Videowand

Die Videowand muss freistehend im Raum positioniert werden. Die angebotene Lösung muss einen sicheren Stand gewährleisten und so konzipiert sein, dass keine elektrischen Anschlüsse freiliegen.

Folgende Punkte muss die Videowand erfüllen:

- Größe mindestens 3,0 m × 1,5 m
- LED Pixel Pitch ca. 0,9 mm ± 0,1mm
- Betriebsdauer ≥ 100.000 h bis L50 oder besser
- Einstellbare Leuchtdichte von 800–1.500 cd/m² ohne Reduzierung der Lebensdauer
- Austausch einzelner Module/Einheiten bei Defekt, möglichst von der Vorderseite
- Redundante Netzteile
- Automatische Helligkeitsregelung bei konstanter Farbwiedergabe
- Betrachtungswinkel > 170° horizontal und vertikal ohne wahrnehmbare Farb- oder Helligkeitsabweichungen
- Kalibrierung und Farbabgleich über die gesamte Fläche
- Keine sichtbaren Bildunterbrechungen oder Fugen im aktiven Bildbereich

10.2 Monitore

Ergänzend zur Videowand sind in drei weiteren Räumen beziehungsweise Teilbereichen Monitore mit schwenkbarer Wandmontage vorzusehen. Die genaue Anzahl, Positionierung und Raumzuordnung ergibt sich aus dem Anhang „Ausstattung Berlin“ beziehungsweise ist im Rahmen der Auftragsklärung zu bestätigen.

Diese müssen folgende Anforderungen erfüllen:

- Mind. 55“
- Auflösung 4K
- Helligkeit ≥500 cd/m² einstellbar

11 Testumgebung

Bevor die Komponenten in den Wirkbetrieb überführt werden können, muss ein minimaler Aufbau in der sogenannten Testumgebung erfolgen. Alle angebotenen Netzwerkkomponenten müssen mindestens einmal dort aufgebaut und getestet werden; ausgenommen hiervon sind Monitore und die Videowand. Um den Betrieb in der Produktivumgebung sicherzustellen, verbleiben die Komponenten in der Testumgebung. So können spätere Updates und vergleichbare Änderungen vor dem Roll-out getestet werden. Da die Testumgebung nicht produktiv ist, ist dies insbesondere bei der Lizenzierung und im Servicevertrag zu berücksichtigen.

12 Beistellungspflichten der Auftraggeberin

Die Auftraggeberin stellt die erforderlichen Räumlichkeiten sowie die notwendigen elektrischen Anschlussleistungen und Kühlkapazitäten bereit. Erforderliche Netzwerkleitungen einschließlich notwendiger Wanddurchbrüche werden nach Abstimmung durch die Auftraggeberin bereitgestellt. Sofern über die eigentliche Videotechnik hinaus Netzwerkkomponenten, beispielsweise Switches, erforderlich sind, ist im Angebot eindeutig auszuweisen, ob diese durch die Auftraggeberin beigestellt oder durch die Auftragnehmerin geliefert werden sollen. Dabei ist zu berücksichtigen, dass eingesetzte Netzwerkhardware dem technischen Betrieb der Auftraggeberin bekannt und betreibbar sein muss.

13 Installation und Inbetriebnahme

Für Arbeiten in sicherheitsrelevanten Bereichen hat die Auftragnehmerin geeignetes Personal einzusetzen. Soweit eine Sicherheitsüberprüfung SÜ2-vPS erforderlich ist, muss diese vor Projektbeginn vorliegen oder rechtzeitig über die Auftraggeberin angestoßen werden. Die Installation vor Ort ist so zu planen und durchzuführen, dass der laufende Betrieb möglichst wenig beeinträchtigt wird. Erforderliche Begleit- oder Aufsichtspersonen der Auftraggeberin sind im Termin- und Einsatzplan zu berücksichtigen.

Die Installation und Inbetriebnahme der gelieferten Hardware/Systems muss die Auftragnehmerin durchführen, unter Berücksichtigung der Beistellungspflichten der Auftraggeberin.

14 Dokumentation und Schulung

Zum Leistungsumfang gehören mindestens folgende Dokumentations- und Schulungsleistungen:

- technische Dokumentation einschließlich finaler Systemarchitektur,
- Betriebs- und Administrationsdokumentation,
- Netz-, Architektur- und Anschlusspläne im As-built-Stand,
- Port-, Protokoll- und Schnittstellenliste,
- Benutzer-, Rollen- und Rechtekonzept,
- Backup-, Restore- und Wiederanlaufanleitung,
- Update-, Patch- und Wartungsanleitung,
- Störungs- und Eskalationshandbuch,
- Konfigurationssicherung und Lizenzübersicht,
- Abnahmeprotokolle und Prüfnachweise,
- sowie rollenbezogene Schulungen für Bedienpersonal, Administration und technischen Betrieb.

Sämtliche Unterlagen sind in deutscher Sprache und in einem bearbeitbaren, gängigen elektronischen Format zu übergeben, soweit dem keine lizenz- oder herstellerbedingten Einschränkungen entgegenstehen.

15 Abnahme

Die Abnahme setzt mindestens den erfolgreichen Nachweis der nachfolgenden Kriterien voraus. Die Auftragnehmerin hat hierfür einen Testfallkatalog mit Prüfschritten, erwarteten Ergebnissen, Nachweisdokumenten und Verantwortlichkeiten vorzulegen.

- vollständige Funktionsfähigkeit der gelieferten Lösung,
- nachgewiesene sichere Netz- und Sicherheitstrennung,
- gleichzeitige Darstellung von mindestens zehn Quellen je Videowand,
- stabile Layoutdarstellung einschließlich Wiederherstellung nach Neustart,
- zentrale Bedien- und Administrierbarkeit einschließlich Rollen- und Rechtekonzept,
- Bereitstellung und Bedienbarkeit des internen Newstickers,
- Nachweis von Monitoring-, Protokollierungs- und Auditfunktionen,
- Nachweis von Fallback- und Wiederanlaufverfahren,
- Integration der vereinbarten Systeme und Schnittstellen,
- Übergabe der vereinbarten Dokumentation,
- Durchführung der vereinbarten Schulungen,
- erfolgreicher Probetrieb beziehungsweise Stabilitätsnachweis.

Der Probetrieb muss über einen vorab festzulegenden Zeitraum unter realitätsnahen Betriebsbedingungen erfolgen. Während des Probetriebs sind insbesondere Stabilität, Bedienbarkeit, Quellenumschaltung, Layoutwechsel, Newsticker, Monitoring, Protokollierung, Wiederanlauf und Störungsverhalten nachzuweisen.

Im Rahmen der Auftragsklärung vor Abnahme sind insbesondere die konkreten Prüffälle je Sicherheitsdomäne, die zulässigen Wiederanlaufzeiten, die Dauer des Probetriebs sowie die konkreten Automatisierungsereignisse abschließend festzulegen. Die standortübergreifende Darstellung ist nicht Bestandteil der initialen Abnahme, sondern als perspektivische Erweiterungsoption zu beschreiben.

16 Betrieb und Support

Nach erfolgter Abnahme geht die Betriebsverantwortung auf die Auftraggeberin über, soweit keine gesonderten Betriebsleistungen beauftragt werden.

Die Auftragnehmerin hat mindestens telefonischen Support während der vereinbarten Servicezeiten anzubieten. Ergänzende oder darüberhinausgehende Supportmodelle sind gesondert auszuweisen.

Sicherheitsrelevante Aktualisierungen und Patches sind regelmäßig sowie anlassbezogen bereitzustellen. Das Verfahren für Patchmanagement, Freigabe und Einbringung ist im Betriebskonzept darzustellen.

Nachfolgenden Service- und Supportmodelle anzubieten oder gleichwertige Serviceklassen nachvollziehbar gegenüberzustellen.

Parameter	Serviceklasse 1	Serviceklasse 2
Servicezeit	24x7x365	7x12
Reaktionszeit	bis 60 Minuten	bis 4 Stunden
Wiederherstellungszeit	48h	72h
Ersatzteilversorgung	Vor-Ort-Vorhaltung oder Regionaldepot	Lagerhaltung mit gesicherter Verfügbarkeit
Software-Updates	inkl. Minor- und Major-Updates	inkl. Major-Updates

17 Zusammenfassung der MUSS Anforderungen

Hier werden die MUSS Anforderungen komprimiert zusammengefasst.

4	Routing-, Bridging- oder Proxyfunktionen zwischen Netzbereichen dürfen nicht vorhanden sein.
4	Die Lösung muss physisch getrennte Air-Gap-Architekturen unterstützen und vollständig On-Premise betreibbar sein.
4	Die Lösung darf keine Cloud-Abhängigkeit besitzen; aktive Funktechnologien dürfen nicht vorhanden sein oder müssen hardwareseitig deaktivierbar sein.
4	Informationen unterschiedlicher Sicherheitsdomänen müssen gleichzeitig auf derselben Videowand dargestellt werden können, ohne die Netztrennung zu beeinträchtigen.
5	Alle zentralen Komponenten, Betriebssysteme, Dienste und Schnittstellen sind nach anerkannten Grundsätzen der IT-Sicherheit zu härten.
5	Nicht benötigte Dienste, Ports, Protokolle, Konten, Funktechnologien und Schnittstellen sind zu deaktivieren oder technisch zu unterbinden.
5	Fernwartung darf nur nach Freigabe erfolgen; Zugänge müssen deaktivierbar, zeitlich begrenzt, eindeutig authentisierbar und vollständig protokollierbar sein.
5	Zugriffsmöglichkeiten von Herstellern, Unterauftragnehmern und Supporteinheiten auf Komponenten, Protokolle, Konfigurationen oder Inhalte sind offenzulegen.
6.1	Flexible Segmentierung, Bild-in-Bild, Kachelansicht und frei platzierbare Fenster müssen unterstützt werden.

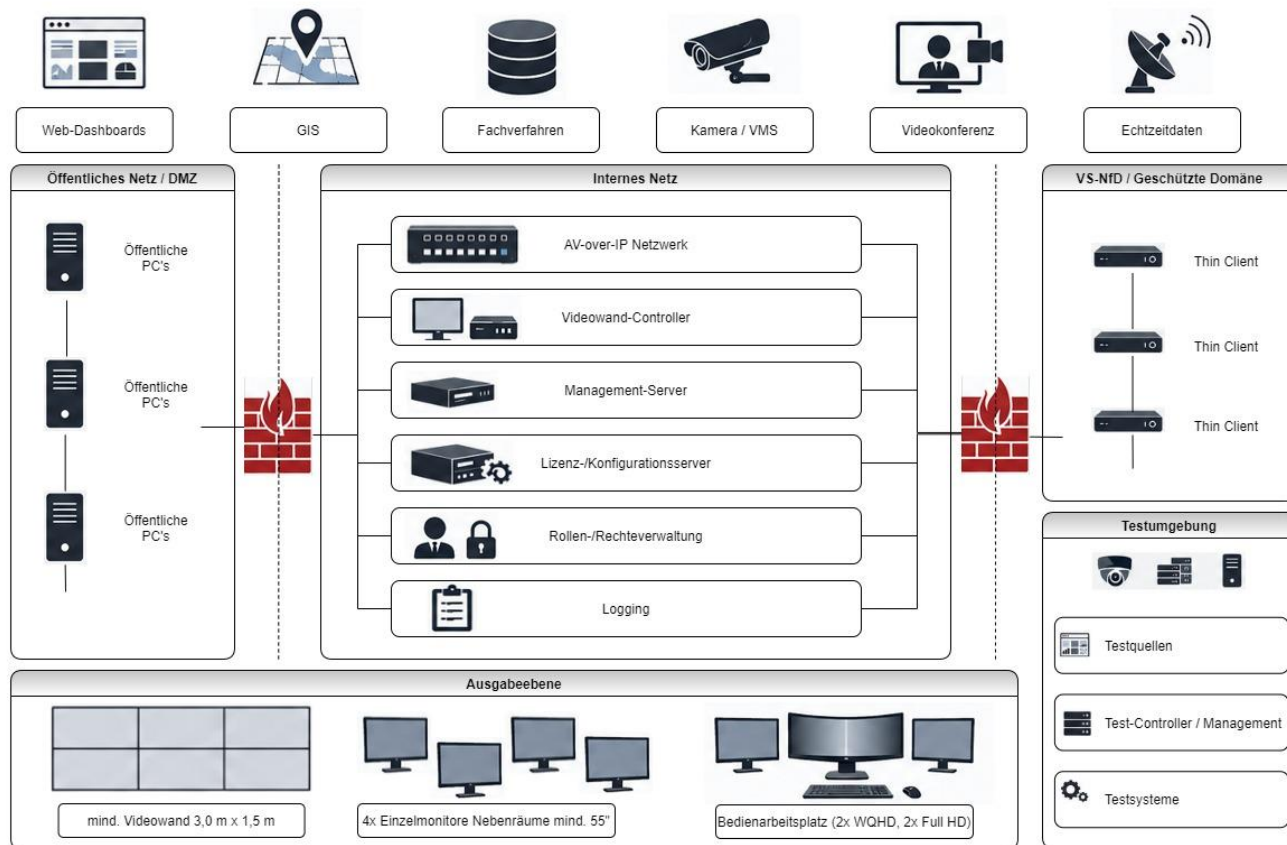
6.1	Je Videowand müssen mindestens zehn voneinander unabhängige Quellen gleichzeitig darstellbar sein.
6.1	Layoutprofile und Szenen müssen gespeichert, versioniert, rollenbezogen bereitgestellt und ohne Neustart aufgerufen werden können.
6.1	Nach Neustart oder Wiederanlauf muss das zuletzt aktive Layout automatisch wiederherstellbar sein.
6.1	Die Lösung muss für eine spätere Erweiterung auf weitere Standorte oder ein zweites Videowandsystem ausgelegt sein.
6.2	Physische, virtuelle und webbasierte Quellen müssen parallel darstellbar, zentral verwaltbar und eindeutig einer Sicherheitsdomäne zuordenbar sein.
6.2	Das bestehende Citrix-/TightGate-Betriebsmodell muss ohne Beeinträchtigung der Netz- und Sicherheitstrennung berücksichtigt werden.
6.3	Das System muss zentral administrierbar und bedienbar sein; lokale Bedienung an Einzelkomponenten darf im Regelbetrieb nicht erforderlich sein.
6.3	Administration, Bedienung, Layout-, Benutzer- und Systemverwaltung müssen rollenbasiert regelbar sein; parallele Bedienung durch mehrere Berechtigte muss möglich sein.
6.3	Die zentrale Bedienoberfläche muss im Betriebsnetz verfügbar sein und ohne Cloud-Dienste funktionieren.
6.3	Mandantenfähigkeit beziehungsweise gruppenbezogene Sichten auf Inhalte, Quellen und Layouts müssen unterstützt werden.
6.3	Mindestens vier berechnete Arbeitsplätze müssen Monitorinhalte oder Anwendungen kontrolliert innerhalb der zulässigen Sicherheitsdomäne übertragen können.
6.4	Die Basislösung muss einen manuell pflegbaren, aktivierbaren und deaktivierbaren internen Newsticker bereitstellen.
6.4	Ereignisbasierte Layoutaufrufe, potenzialfreie Kontakte und ergänzende Signalisierungen müssen unterstützt werden.

6.4	Ereignisse unterschiedlicher Kritikalität müssen visuell unterscheidbar dargestellt werden können.
7	Die Lösung ist für 24/7-Betrieb auszulegen; der Ausfall einzelner Teilkomponenten darf nicht zum vollständigen Verlust der Visualisierungsfähigkeit führen.
7	Backup-, Wiederanlauf- und Wiederherstellungsmechanismen sind bereitzustellen und zu dokumentieren.
7	Redundanzoptionen für zentrale Komponenten, Netzteile, Steuerung, Zuspelwege und Management sind mit Auswirkungen darzustellen.
7	Das System muss ohne Austausch zentraler Komponenten hinsichtlich Monitoren und Mitarbeiterplätzen modular erweiterbar sein.
8	Die Lösung muss über standardisierte oder dokumentierte Schnittstellen in Betriebs- und Sicherheitsmonitoring integrierbar sein.
8	Verfügbarkeit, Komponentenstatus, Netzteile, Lüfter, Temperatur, Auslastung, Quellen, Lizenzen, Speicher und Kommunikationswege müssen überwachbar sein.
8	Sicherheitsrelevante Ereignisse müssen über geeignete Schnittstellen an ein zentrales SIEM übergeben werden können.
8	Protokolldaten müssen exportierbar, auswertbar und hinsichtlich Aufbewahrung, Formaten, Zeitquelle und Manipulationsschutz beschrieben sein.
10	Die Hardware muss für professionellen 24/7-Betrieb geeignet sein; alle netzwerkfähigen Komponenten müssen IPv4 und IPv6 unterstützen.
10.1	Die Videowand muss freistehend, standsicher und ohne freiliegende elektrische Anschlüsse ausgeführt werden.
10.1	Größe mindestens 3,0 m × 1,5 m; Pixel Pitch ca. 0,9 mm ± 0,1 mm; Betriebsdauer mindestens 100.000 h bis L50 oder besser.
10.1	Leuchtdichte 800–1.500 cd/m ² einstellbar, redundante Netzteile, automatische Helligkeitsregelung, Betrachtungswinkel größer 170°, Kalibrierung und fugenfreie Bilddarstellung.

10.2	Monitore müssen mindestens 55 Zoll, 4K-Auflösung und eine einstellbare Helligkeit von mindestens 500 cd/m ² aufweisen.
-------------	---

Anhang

Netzwerkarchitektur für Leitstellen- & Lagezentren



Platzierung Videowände und Monitore

