



Leistungsverzeichnis

Projekt zur Erprobung KI-gestützter Videotechnik im
Objektschutz der Polizei Berlin



Inhaltsverzeichnis

ABKÜRZUNGSVERZEICHNIS	4
1 GEGENSTAND	5
2 LEISTUNGSUMFANG	5
3 ALLGEMEINE SYSTEMANFORDERUNGEN (PUNKT 1 DER BEWM)	6
3.1 BETRIEBSANFORDERUNGEN	6
3.2 DOKUMENTATION UND SPRACHE	6
4 FUNKTIONALE ANFORDERUNGEN AN DIE SOFTWARE	6
4.1 KI-ANWENDUNG (PUNKT 2 DER BWM)	6
4.1.1 Objektdetektion, Klassifizierung	6
4.1.2 Detektionsszenarien	7
4.1.3 Alarmverarbeitung	7
4.1.4 Biometrik und Akustik	8
4.1.5 Zuverlässigkeit, Fehlerrate	8
4.1.6 Testphase	8
4.2 VIDEO-MANAGEMENT-SYSTEM (VMS) (PUNKT 3 DER BEWM)	8
4.2.1 Begriffe und Architekturprinzip	8
4.2.2 VMS-Live-Betrieb (Anzeige, Recherche, Arbeitsablauf)	9
4.2.3 Versammlungslagen innerhalb des Schutz- und Beobachtungsbereichs ...	12
4.3 MOBILE EINHEITEN	12
4.3.1 Optionales Drohnenmodul	13
5 FUNKTIONALE ANFORDERUNGEN AN DIE HARDWARE (PUNKT 4 DER BEWM) ...	13
5.1 KAMERA-KONZEPT	13
5.1.1 technische Angaben	13
5.1.2 Visualisierung	14
5.1.3 Genehmigungsvorbehalt	14
5.2 KI- UND VMS-SERVER	15
5.3 VMS-ARBEITSPLATZ / VIDEOAUSWERTUNG	16
5.3.1 Arbeitsplatztisch	16
5.3.2 VMS-Client-Rechner	16
5.3.3 Eingabe- / Audiogeräte	16
5.4 MOBILE EINHEITEN	16
6 NICHT-FUNKTIONALE ANFORDERUNGEN (PUNKT 5 DER BEWM)	17
6.1 VERFÜGBARKEIT, LEISTUNG, REDUNDANZ	17
6.2 SKALIERBARKEIT	17
6.3 EXPORTE / SCHNITTSTELLEN	18
6.4 UNTERSTÜTZTE STREAMING-FORMATE / AUDIO- UND VIDEO-CODECS	18
6.5 LOGGING / PROTOKOLLE	19
6.6 UPDATES / CHANGE-MANAGEMENT	19

6.7	USABILITY / GUI.....	20
6.8	MONITORING	20
6.9	SUPPORT.....	20
7	SCHULUNGEN (A).....	21
7.1	ANFORDERUNGEN AN SCHULUNGEN.....	21
7.2	ANFORDERUNGEN AN SCHULUNGSUNTERLAGEN	22
7.3	SCHULUNG ANWENDER/MULTIPLIKATOREN.....	22
7.4	SCHULUNG SYSTEMADMINISTRATOREN	23
7.4.1	Bedienung der Module (Software, Hardware)	23
7.4.2	Wartung und Instandsetzung	23
7.4.3	Zusätzliche Inhalte angepasst auf Ebene des 2nd-Level-Supports:.....	23
8	KONZEPTE.....	24
9	SLA - SERVICE LEVEL AGREEMENTS	24
10	RICHTLINIEN ZUR SYSTEMTECHNIK	24
10.1	LAN-SECURITY 802.1X (AUTHENTICATION).....	24
10.2	IPV6.....	24
11	LIZENZEN (A).....	25
11.1	LIZENZBEDINGUNGEN.....	25
11.2	LIZENZLAUFZEIT	25
11.3	ANZAHL DER LIZENZEN	25
11.4	RECHTS- UND HAFTUNGSFRAGEN.....	25
11.5	SICHERHEITS- UND DATENSCHUTZANFORDERUNGEN.....	25
11.6	EINSCHRÄNKUNGEN UND SONDERBEDINGUNGEN	25
11.7	MIGRATION UND INTEROPERABILITÄT	25
11.8	LIZENZMANAGEMENT	26
12	ANHÄNGE	26

Abkürzungsverzeichnis

AG	Auftraggeber
AD	Active Directory
AN	Auftragnehmer
API	Application Programming Interface
BewM	Bewertungsmatrix
GUI	Graphical User Interface
HW	Hardware
LV	Leistungsverzeichnis
OU	Organizational Unit
PRTG	Paessler Router Traffic Grapher
PKI	Public Key Infrastruktur
RDBMS	Relationales Datenbankverwaltungssystem
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SW	Software
UCD	User-Centered Design
UID	Unique Identifier
VMS	Video-Management-System
WEEE	Waste of Electrical and Electronic Equipment

1 Gegenstand

Gegenstand dieses Leistungsverzeichnisses ist die Beschaffung von intelligenter Videotechnik im Rahmen des § 24a ASOG Berlin und Begleitvorschriften, um vor einer weiterreichenden Implementierung deren Eignung für den Einsatz im Objektschutz der Polizei Berlin zu erproben. Hierfür sollen 2 Pilotobjekte mit entsprechender – grundsätzlich fest installierter – Technik ausgestattet werden. Bei diesen Objekten handelt es sich zum einen um das Alte Stadthaus (Dienstszitz der Senatsverwaltung für Inneres und Sport – SenInnSport) in 10179 Berlin, Klosterstr. 47 und zum anderen um das Berliner Rathaus (Dienstszitz des Regierenden Bürgermeisters von Berlin und der Senatskanzlei) in 10178 Berlin, Rathausstr. 15.

An einem weiteren Objekt sollen mobile Lösungen erprobt werden. Bei diesem Objekt handelt es sich zunächst um das Abgeordnetenhaus von Berlin (Sitz des Landesparlaments) in 10117 Berlin, Niederkirchnerstr. 5. Sollte sich im Rahmen des behördlichen Genehmigungsverfahrens herausstellen, dass die Installation an einem der genannten Objekte nicht realisiert werden kann bzw. einzelne Objekte aufgrund von Einwänden des Objekthalters gar nicht mehr als Pilotobjekte zur Verfügung stehen, behält sich der AG vor, kurzfristig entsprechende Ersatzobjekte zu benennen oder den Einsatz mobiler Technik an den oben benannten Standorten zu beauftragen (zum Genehmigungsvorbehalt siehe 5.1.3).

Die genannten Pilotobjekte sollen grundsätzlich alle im Jahr 2026 mit entsprechender Technik ausgerüstet werden. Der AG behält sich jedoch vor, einzelne Objekte erst in 2027 auszurüsten, sowie das Projekt gegebenenfalls auf weitere Pilotobjekte auszuweiten.

Die Erprobung gliedert sich in eine 3-monatige Testphase und einen sich anschließenden 9-monatigen Probebetrieb.

2 Leistungsumfang

Der Auftragnehmer (AN) hat ein vollständig integriertes System als Gesamtpaket zu liefern. Dabei sind die sicherheitsrelevanten, funktionalen, betrieblichen und organisatorischen Anforderungen des Auftraggebers (AG), so wie in diesem Leistungsverzeichnis und der dazugehörigen Bewertungsmatrix dargestellt, zu erfüllen. Der Leistungsumfang umfasst insbesondere folgende Komponenten:

- stationäre und mobile Videoeinheiten sowie optional Drohnensysteme,
- KI-Analyse-Software,
- VMS-Software in Client-/Server-Architektur,
- Einen Leitstellen-Arbeitsplatz einschließlich Peripheriegeräten in ergonomischer Ausstattung,
- Mechanismen zur Datenschutz- und Sicherheitsgewährleistung,
- Dienstleistungen für Betrieb, Wartung, Support und Schulung,
- vollständige technische Dokumentationen.

Der AN schuldet die vollständige funktionsfähige Gesamtlösung, einschließlich Installation, Integration, Parametrisierung, Test, Schulung und Übergabe in den Pilotbetrieb.

3 Allgemeine Systemanforderungen *(Punkt 1 der BewM)*

3.1 Betriebsanforderungen

Das VMS muss vollständig im Rechenzentrum des AG betreibbar sein (On-Premise-Lösung). Alle Betriebs-, Sicherheits- und Updatefunktionen müssen im Offline-Betrieb verfügbar sein. Das System darf nicht von Cloud-Diensten abhängig sein. Die Betriebsfähigkeit muss durch geeignete Maßnahmen gegen externe Störungen und Netzausfälle sichergestellt werden.

3.2 Dokumentation und Sprache

Der AN stellt eine vollständige Dokumentation bereit, darunter:

- Benutzer- und Administrationshandbücher,
- technische Integrationsdokumentationen,
- Schnittstellenbeschreibungen,
- Schulungsunterlagen,
- Dokumentation zu Hardwarekomponenten.

Sämtliche Benutzeroberflächen, Protokollmeldungen, Fehlermeldungen, Logeinträge, Supportkommunikation und Dokumentationen sind vollständig in deutscher Sprache zu gestalten. Dokumente/Handbücher sind digital im Portable Document Format (PDF) bereitzustellen. Alle Dokumente/Handbücher sollen auch ohne Internetzugang nutzbar sein.

4 Funktionale Anforderungen an die Software

4.1 KI-Anwendung *(Punkt 2 der BwM)*

4.1.1 Objektdetektion, Klassifizierung

- Die KI detektiert, klassifiziert/identifiziert und lokalisiert Objekte, Personen und Szenarien im Bild.
- Die KI muss Objektdetektion und Klassifizierung nach mehreren Merkmalen unterstützen (z. B. Person, Fahrzeugart, Farbe, Kopfbedeckung, Tasche/Rucksack).

4.1.2 Detektionsszenarien

Folgende essenzielle Szenarien müssen/sollen in der kompletten Schutz- und Beobachtungsbereiche (siehe Anhang 6) durch KI-basierte Videoauswerteverfahren detektiert werden:

Perimeter- und Zonenverletzung

- Betreten gesperrter Bereiche
- Überschreiten virtueller Linien (Alarmauslösung nur bei definierten Linien unter Berücksichtigung der Richtungsangabe)
- Klettern auf Zäune/Mauern
- Tailgating
- Anhaltende, beeinträchtigende Lärmeinwirkung (z. B. > 85 dB(A) über > 10 Sek.)
- Audio-Hinweis: Akustische Schwellwertanalyse liefert Hinweise auf Quelle z.B.:
 - Schusswaffengebrauch
 - Detonationen

Objekteinwürfe und Vandalismus

- Werfen von Gegenständen (Steine, Flaschen, Brandsätze)
- Beschädigung von Zäunen, Toren und Vergleichbarem → **MUSS**
- Anbringen von Graffiti/Farbe: Sprüh-/Schmierhandlungen bzw. gleichartige Angriffe in der nahen Objektzone
- Lichtprojektionen

Ungewöhnliche Objektablagen und Verhaltensauffälligkeiten

- Zurückgelassene Gegenstände: Objektgröße > 30 cm und Objektklasse (Feuerlöscher, Tasche, Koffer, Rucksack); Verweildauer ≥ 30 s innerhalb der Zone → Alarm) → **MUSS**
- Unzulässiges Abstellen von Objekten (Fahrzeuge, Fahrräder, Gepäck etc.) in Sicherheitsbereichen → **MUSS**
- Langes Verharren/Umhergehen ohne Anlass
- Langanhaltendes Fotografieren
- Anbringen/Entwenden von Objekten
- Diebstahlhandlungen (z. B. an Fahrrädern)
- Wiederholtes Erscheinen (ohne biometrische Identifikation)

4.1.3 Alarmverarbeitung

- Die KI-Videoanalyse verarbeitet stets den vollständigen Kamera-Stream
- Werden definierte Szenarien erkannt, wird ein Alarm ausgelöst und das erkannte Ereignis unverzüglich an das VMS gesendet (*zu notwendigen Pflichtangaben siehe 4.2.2 - VMS-Live-Betrieb - Verhalten bei Detektion/Alarm*).

Visuelle Alarmdarstellung

- Der Detektionsbereich wird im Bild als Overlay (farbige Bounding Box oder Polygon) markiert – in der Aufzeichnung, kurzzeitig im Live-Bild sowie im Export.
- Das Einblenden der Overlays erfolgt durch das VMS.
- Jeder Alarm enthält den konkreten Auslösegrund in Klarschrift, möglichst mit weiteren Angaben wie z. B. Objektklasse (Feuerlöscher, Tasche, Koffer).

4.1.4 Biometrik und Akustik

- Biometrische Identifizierung (Echtzeit und Archiv) ist ausgeschlossen.
- Die akustische Schwellwertanalyse kann ausschließlich als Hinweis in die Alarmkette einfließen (datenschutzkonform parametrisiert).

4.1.5 Zuverlässigkeit, Fehlerrate

- die KI-gestützte Videoanalyse muss mit einer Gesamterkennungsgenauigkeit von mindestens $\geq 95\%$ operieren.
- Die maximale durchschnittliche Fehlalarmrate soll nicht höher als 25 % über alle Szenarien liegen.

4.1.6 Testphase

Die in der Testphase erlangten Erkenntnisse sollen genutzt werden, um die verwendeten KI-Verfahren qualitativ zu verbessern und die Fehlalarmquote zu verringern.

Dazu werden dem AN die von der KI falsch als Alarm detektierten Ereignisse (False-Positive) für das Nachtrainieren der KI im Rahmen der rechtlichen Zulässigkeit zur Verfügung gestellt. Dabei ist folgendes zu beachten:

- Human-in-the-Loop-Prinzip (keine selbstlernende KI)
- Sicherstellung diskriminierungsfreier Algorithmen¹
- Der Workflow zur Übertragung der Datensätze vom AG an den AN wird im Rahmen des Testbetriebes zwischen beiden Parteien abgestimmt.

Die Möglichkeit das verwendete KI-Verfahren anhand der Erkenntnisse aus der Testphase zu trainieren, ist ein bewertungsrelevantes Kriterium. *(siehe 2.3.3 der Bewertungsmatrix)*

4.2 Video-Management-System (VMS) *(Punkt 3 der BewM)*

4.2.1 Begriffe und Architekturprinzip

Das Video-Management-System (VMS) bildet die zentrale Bedien-, Anzeige- und Rechercheplattform für Alarme, Livebilder, Wiedergaben und Exporte. Das System bietet

¹ Es ist darzulegen, wie dies erreicht wird

eine Benutzeranmeldung. Diese soll an das beim AG betriebene Active-Directory-Umgebung (AD) angebunden werden können.

Zonen- und Linienlogik

- Zonen und Linien werden **ausschließlich im VMS** definiert, verwaltet und versioniert.
- Für jedes von der KI gemeldete Ereignis prüft das VMS, ob sich der Detektionsbereich innerhalb einer definierten Zone oder Linie befindet. Nur dann wird ein Alarm erzeugt; Ereignisse außerhalb definierter Bereiche werden verworfen.
- Ein Richtungsbezug ($A \rightarrow B$ / $B \rightarrow A$) darf nur dort angewendet werden, wo das jeweilige Szenario fachlich eine Richtungsabhängigkeit erfordert. Ein bloßes Ein- oder Austreten in eine Zone löst standardmäßig keinen Alarm aus.
- Bei sicherheitsrelevanten Szenarien wie z. B. Tailgating, Betreten von sicherheitsrelevanten oder gesperrten Bereichen, unzulässigem Verlassen gesicherter Bereiche muss ein Alarm ausgelöst werden.

Systemarchitektur

- VMS und KI sind fachlich und funktional getrennt zu betrachten.
- Das VMS muss stationäre, mobile, temporäre und mehrere geografisch getrennte Installationen (**Multi-Site-Umgebungen**) zentral verwalten und synchronisieren können.
- Die Systemarchitektur hat sicherzustellen, dass **Live, Wiedergabe, Analyse** und **Export** gleichzeitig auf unterschiedlichen Bedien-Clients ausführbar sind, ohne dass Systemwechsel oder zusätzliche Programme erforderlich sind.
- Pre-Recording bezeichnet die automatische Sicherung eines Vorlaufs vor dem Ereignis.
- PTZ-Kameras dienen der lagegerechten Aufklärung im Ereignisfall.

4.2.2 VMS-Live-Betrieb (Anzeige, Recherche, Arbeitsablauf)

Bedienoberfläche und Recherchefunktionen

- Das VMS hat mehrere parallel nutzbare Video-Layouts (z. B. Multi-Split, Quad, benutzerdefiniert) zu unterstützen, die durch den Bediener jederzeit dynamisch gewechselt werden können.
- Live-Ansicht, Wiedergabe und forensische Recherche müssen in einer einheitlichen Bedienoberfläche erfolgen; getrennte Anwendungen sind unzulässig.
- Das System muss Suchfunktionen nach Zeit, Attributen, Objekten oder Alarmklassen bereitstellen.

- Eine synchrone Suche und Wiedergabe über mehrere Kameras auf einer gemeinsamen Zeitleiste ist erforderlich – auch wenn diese auf unterschiedlichen Aufzeichnungsservern liegen.
- Das System muss eine forensische Suche nach Attributen und Ähnlichkeitsmerkmalen (Objekte, Farben, Größen, Bewegungsrichtung) in Live- und Archivbildern ermöglichen.
- Suchergebnisse müssen in einer kombinierten Tabelle und Videovorschau angezeigt werden; ein direkter Sprung zur Aufnahme muss möglich sein.
- Jede manuelle Kameraumschaltung ist mit Benutzerkennung, Zeitstempel und Kamera/Ansicht zu protokollieren.

Mehrmonitorbetrieb

- Weitere Monitore am Arbeitsplatz müssen jederzeit manuell für Live- oder Rechercheansichten aktiviert werden können.
- Mehrmonitor-Layouts müssen eine klare Trennung von Überblick und Detail/Recherchedarstellung ermöglichen.

PTZ-Funktionalität

- PTZ-Kameras sind vollständig im VMS manuell steuerbar.
- Eine automatische PTZ-Ausrichtung darf nicht erfolgen; nur explizite Operator-Kommandos sind zulässig.
- Nicht betroffene Kameras verharren in ihrer Wachposition.

Overlays, Vor-/Nachlauf, Export

- Overlays (Bounding Box/Polygon) sind gemäß den von der KI gelieferten Pixelkoordinaten in Live, Wiedergabe und Export darzustellen.
- Das VMS stellt Pre-Recording (Vorlauf ≥ 60 s) sowie Nachlauf bereit und ruft diese bei Alarm automatisch ab.
- Exporte müssen einen Integritätsnachweis enthalten.

Maskierung

- Maskierungen/Verpixelungen von Bereichen oder Objekten, die nicht überwacht werden dürfen oder sollen, müssen möglich sein – sowohl bei statischen als auch bei PTZ-Kameras.
- Maskierungen müssen in Live, Wiedergabe und Export wirksam sein.

Interaktive Karten- und Objektanzeige

Das VMS muss eine interaktive Karten- und Objektansicht bereitstellen mit:

- Anzeige aktiver Kameras, Zonen und Alarmpositionen,
- direkter Umschaltung der entsprechenden Kamera per Klick auf das Symbol,

- klarer räumlicher Zuordnung der Ereignisse.

Verhalten im Normalbetrieb (kein detektiertes Ereignis)

Der Live-Betrieb des VMS muss einen **anlassbezogenen Regelbetrieb** unterstützen. Im Normalzustand zeigt das System auf dem Ereignis-/Alarmmonitor eine reduzierte Darstellung („schwarzer Monitor“) ohne permanente Livebilder. Ein manuelles alarmunabhängiges Umschalten einzelner Kameras ist jedoch möglich.

Verhalten bei Detektion / Alarm

Bei einem von der KI gemeldeten und vom VMS validierten Ereignis (*vgl. Abschnitt 4.1.2*) muss das System automatisch:

- die betroffene Kamera umschalten,
- die Position des Ereignisses in der Karte anzeigen,
- den direkten Zugriff auf die Aufzeichnung zum Zeitpunkt der Detektion ermöglichen (inkl. Vor-/Zurückspulen innerhalb der Szene),
- folgende Pflichtangaben darstellen:
 - o Auslösegrund,
 - o betroffene/auslösende Kamera,
 - o referenzierte Zone/Linie,
 - o Zeitstempel,
 - o Detektionsbereich im Bild (Overlay: Bounding Box oder Polygon),
 - o ggf. angewandter Richtungsfilter
- Mehrere Alarme werden parallel angezeigt (tabellarische Darstellung)
- Keine Unterdrückung weiterer Alarme, auch nicht bei noch offenen unbearbeiteten Alarmen
- Alle Alarme müssen in einer Übersicht dargestellt werden, idealerweise in tabellarischer Form.
- Ein Direktsprung von der Alarmzeile in die betroffene Ansicht sowie die synchronisierte Parallelsichtung mehrerer Kameras muss möglich sein.
- Die Bearbeitungsreihenfolge wird vom Bedienpersonal festgelegt.
- Alarme müssen nach Kategorie, Quelle, Ereignistyp und Ursprungsgerät gefiltert werden können.
- Die Alarme müssen kategorisiert werden können, mindestens in die Kategorien „offen“ (Standard bei Eintreffen eines KI-Alarms) und „geschlossen“; weitere optionale Kategorien wie z. B. „in Bearbeitung“ sind wünschenswert.
- Jeder Alarm ist quittierungspflichtig und ohne Systemwechsel in die Maßnahmenbearbeitung zu überführen.

soll das System automatisch:

- statische Nachbaransichten (ohne Mitschwenken weiterer PTZ) zuschalten.

- Das VMS muss eine regelbasierte Weiterleitung und Aggregation von Alarmen an übergeordnete Leitstellen unterstützen.
- Alle Alarmereignisse müssen mit dazugehörigen Video- und Metadaten verknüpft sein und direkt innerhalb des VMS abrufbar bleiben.
- Vom Operator als False-Positive deklarierte Alarmereignisse müssen mit dazugehörigen Video- und Metadaten aus dem VMS heraus an einem separaten Speicherort abgelegt, von dort wieder abgerufen und exportiert werden können (siehe 4.1.6 Testphase).
- Menschliche Aufsicht:
 - o Entscheidungen der KI unterliegen menschlicher Kontrolle,
 - o Keine vollautomatisierten Maßnahmen ohne Bedienerbestätigung,

4.2.3 Versammlungslagen innerhalb des Schutz- und Beobachtungsbereichs

Das System muss eine „Versammlungsschaltung“ enthalten, welche durch den Operator für einzelne Kameras oder ganze Zonen aktiviert und deaktiviert werden kann.

- Im Regelbetrieb, ohne Versammlungslagen
 - o Versammlungsschaltung im Modus „Inaktiv“
 - o Das System arbeitet mit den festgelegten Parametern
- Beim Vorliegen einer Versammlungslage
 - o Versammlungsschaltung im Modus „Aktiv“
 - o Sämtliche Detektionen und Alarm-Meldungen werden unterdrückt
 - o Es finden keine Aufzeichnungen durch die betroffenen Kameras statt.

Der aktuelle Zustand und jede Umschaltung (von inaktiv in aktiv und umgekehrt) müssen im VMS visualisiert werden. Jede Umschaltung ist revisionssicher (Nutzerkennung, Zeitstempel, Zone, Zustand) mittels Logfile zu protokollieren.

4.3 Mobile Einheiten

Das System ermöglicht den gleichzeitigen Betrieb mehrerer mobiler Knoten innerhalb derselben Zonenstruktur mit identischen Alarmierungsregeln.

Mobile Einheiten binden sich verschlüsselt in das VMS ein und folgen denselben Bedienmustern wie die stationären Lösungen.

- Standard muss der anlassbezogene Regelbetrieb ohne Dauer-Livebild auf dem Ereignis-Monitor sein
- Manuelles Einschalten weiterer Monitore muss möglich sein und geloggt werden.
- Es müssen ebenfalls alle KI-Videoauswertungsverfahren, die in Abschnitt 4 definiert sind, ausgeführt werden.
- Zonen/Linien, Pre-Recording, Maskierung, Overlay, Export-Integrität und vollständiges Logging müssen identisch gelten. Kommunikation muss über gesicherte Verbindungen (z. B. VPN via 4G/5G/WLAN) erfolgen.

- Alarmer müssen gleichrangig in der VMS-Alarmanzeige erscheinen und werden identisch quittiert/bearbeitet.
- Mobile Einheiten müssen auch temporäre oder ad-hoc Kameras automatisch in das VMS-Layout integrieren können.

4.3.1 Optionales Drohnenmodul

Es soll ein optionales Drohnen-Modul angeboten werden, welches in die mobile Lösung integrierbar ist. Dabei sind folgende Funktionen zu erfüllen:

- Ereignis- oder operatorgesteuerter Start;
- Bereichsflug entlang Geofences/Routen;
- Rückkehr-/Abbruchlogik sowie Protokollierung jeder manuellen Steuerung (Nutzer, Zeit, Einsatzraum);
- Video-Stream ins VMS mit den gleichen Zonen-, Overlay- und Maskierungsfunktionen wie bei den stationären Lösungen;
- Regeln für Export-Integrität und Logging gelten entsprechend.

5 Funktionale Anforderungen an die Hardware *(Punkt 4 der BewM)*

5.1 Kamera-Konzept

- Jede Kamera sollte dem System mehrere (idealerweise drei) verschiedene Videoströme gleichzeitig zur Verfügung stellen, sodass beispielsweise
 - o ein hochauflösender Stream für die beweissichere Archivierung,
 - o ein optimierter (und ggf. komprimierter) Stream für die laufende KI-Analyse sowie ein
 - o zusätzlicher Stream für z. B. eine Live-Übersicht oder spezielle Arbeitsplätze
 separat genutzt werden können.
- Es ist sicherzustellen, dass die Bildrate und Qualität des für die KI-Analyse vorgesehenen Streams mindestens FullHD sowie eine ausreichend hohe Bildwiederholrate aufweist – insbesondere für Szenarien mit schneller Bewegung wie Flaschenwurf.
- Die Kompression beim KI-Analyse-Stream darf die Detektionsfähigkeit nicht beeinträchtigen.
- Ist ein dritter Stream nur in reduzierter Qualität (z. B. für die Übersicht) möglich, kann dieser genutzt oder – sofern technisch erforderlich – mittels Transcodierung im System erzeugt werden.

5.1.1 technische Angaben

Für jedes Objekt ist eine ausführliche Kamera-Einsatzplanung zu erstellen, die zunächst von einer Installation an der Gebäudehülle ausgeht. In dieser Planung sind für jede Kamera mindestens folgende Parameter darzustellen:

- Art der Kamera (statisch / PTZ)
 - o Hersteller
 - o Modell
 - o Verwendete Sensorik (IR, NIR, Low-Light etc.)
 - o Brennweite
- Auflösung in Megapixel
- Detektionsreichweiten in Metern
- Detektionsgrößen in Pixel
- Befestigungsart und -ort
 - o Befestigungstechnik und -material
 - o Installationsort und -höhe (Bemaßungsskizzen für jede Gebäudeseite)
- Anbindung an die gebäudeseitige IT- und Netz-Infrastruktur

Für das Gesamtsystem ist die durchschnittlich zu erwartende Leistungsaufnahme in kW/h sowie die benötigte Bandbreite für die Übertragung der Videosignale zum VMS-Server anzugeben. Darüber hinaus ist darzustellen, wie die Vorgabe, dass die Kameras auch bei schlechten Lichtverhältnissen ausreichende Bildauflösungen erreichen, technisch umgesetzt wird.

5.1.2 Visualisierung

Die mit der geplanten Technik erreichbaren Abdeckungsbereiche sind in einer grafischen Darstellung (3D) zu visualisieren. Hierbei sind die baulichen Besonderheiten der Objekte (Mauervorsprünge, Tor-/Türnischen, Hofeinfahrten, Gräben etc.) und deren technische Berücksichtigung besonders hervorzuheben. Lage und Ausmaß von „Blinden Flecken“ (Sichthindernisse/Abschattungen) sind nachvollziehbar darzustellen.

5.1.3 Genehmigungsvorbehalt

Es wird ausdrücklich darauf hingewiesen, dass die Realisierbarkeit des Kamera-Konzepts unter dem Vorbehalt der Genehmigung durch die Denkmalschutz-Behörde steht. Eine grundsätzliche Zustimmung bzw. Rahmenvorgaben werden ohne das Vorliegen eines konkreten Konzeptes seitens der Denkmalschutz-Behörde abgelehnt. Gleicher Vorbehalt gilt für die jeweiligen Objekthalter (zur Einbindung der Denkmalschutzbehörde siehe Beschreibung der Auswertungssystematik Punkt 2.4).

Die Anbieter haben daher vorsorglich neben den Kamera-Konzepten für eine Installation an der Gebäudehülle Alternativen für eine davon unabhängige Installation im Umfeld der Schutzobjekte zu liefern. Für diese Alternativen gelten die unter 5.1.1 genannten Anforderungen entsprechend.

5.2 KI- und VMS-Server

- Für alle kritischen Komponenten (VMS-Server und KI-Server) ist eine Redundanz durch mindestens zwei unabhängige physische oder virtuelle Systeme vorzusehen. Die Redundanz kann gestaltet werden als:
 - Active-Standby-Konfiguration (ein System arbeitet aktiv, ein identisch ausgestattetes System steht als Hot-Standby bereit und übernimmt bei Ausfall unmittelbar)oder
 - als Active-Active-Konfiguration (beide Systeme sind zeitgleich aktiv und teilen sich die Aufgaben/-Last, bei Ausfall übernimmt das verbleibende System alle Funktionen)realisiert werden.
- Im Fehlerfall (Ausfall eines Servers oder wesentlicher Hardwarekomponenten) muss der Betrieb vollautomatisch für alle Kernfunktionen (Aufzeichnung, Alarmierung, Analyse, Steuerung) ohne Datenverlust oder signifikante Unterbrechung fortgesetzt werden.
- Für alle Systemdaten, Konfigurationen und Echtzeitalarme ist eine synchronisierte Spiegelung/Failover zu gewährleisten.
- Der Schwenk auf die redundanten Ressourcen darf eine Gesamtdauer von maximal 2 Minuten nicht überschreiten.
- Die Überwachung und Statusanzeige aller Redundanzpfade kann zentral im VMS dargestellt und protokolliert werden, sofern diese Komponenten (z. B. VMS-Server, direkt angebundene GPU-Server) vom VMS verwaltet oder integriert sind.
- Bei extern eingebundenen oder von Drittanbietern betriebenen KI-Servern und -Verfahren ist eine Status- oder Alive-Meldung ausreichend.
- Speicher/NVR für Daueraufzeichnung + ereignisbezogene Clips gemäß Speicher-/Löschkonzept.
- Gesicherte Netzanbindung (z. B. VLAN/VPN) zwischen Kameras, KI-Server und/oder Embedded Devices, VMS-Server und Leitstelle.
- KI-Videoauswertung muss auf GPU-Server/n (KI-Server) im Rechenzentrum der Polizei Berlin oder auf den Kameras oder Embedded Devices ausgeführt werden;
- eine Ausführung der KI-Videoauswertung in der Cloud ist nicht erlaubt.
- Die Nicht-Funktionalen Anforderungen wie Detektionsrate etc. müssen dabei erreicht werden
- Der VMS-Server muss sich im polizeilichen Rechenzentrum befinden;
- VMS-Client-PCs als Arbeitsplatz (VMS-Arbeitsplatz)
- Es muss die Möglichkeit bestehen, durch direkte Streaming-Verbindungen zwischen Kamera und Client eine Lastreduktion beim Server herbeizuführen

5.3 VMS-Arbeitsplatz / Videoauswertung

5.3.1 Arbeitsplatztisch

- Zwei hochauflösende Ultra-Wide- oder Extended-Ultra-Wide-Curved-Displays ≥ 57 Zoll im Format **mindestens 21:9, alternativ $\geq 21:10$ / $21:11$** (mindestens 4K-äquivalent über die gesamte Breite)
 - oben Ereignis-/Alarm-Bildschirm - „Schwarzer Monitor“ (Übersichtsdarstellung bei Alarmauslösung)
 - unten Detail/Recherche (zeitachsensynchrone Sichtung).
 - Nur der Ereignis-/Alarm-Bildschirm schaltet bei Detektion automatisch ein;
 - weitere Monitore sind jederzeit manuell zuschaltbar (mit Protokoll).
- höhenverstellbare Monitor-Halterung für vertikale Montage
- Ergonomischer Leitstellentisch für 24/7-Betrieb
 - Elektrisch höhenverstellbar (65-125 cm)
 - Mindestmaße der Tischplatte: $\geq 220\text{cm}$ breite, $\geq 100\text{cm}$ Tiefe (optimierter Betrachtungsabstand für geforderte Monitore - 80cm nicht ausreichend)
 - Integrierte Kabel-/Technikkanäle für diskrete Verkabelung von Monitoren und sonstigen Peripherie-Geräten

5.3.2 VMS-Client-Rechner

- Gleichzeitige Ausgabe beider Widescreens mindestens in 4K inkl. flüssiger Wiedergabe mehrerer Streams (HW-Beschleunigung für H.264/H.265);
- Störungsfreie mehrfach-Stream-Dekodierung (gleichzeitig Live + Playback + Pre-Recording-Clip)
- Netzwerk-Redundanz (2× LAN/NIC) für Ausfalltoleranz am Platz
- Platznaher Technik-/Client-Container mit Geräuschkämmung und passiver Kühlung.

5.3.3 Eingabe- /Audiogeräte

- Eingabegeräte im Standard-Layout (Tastatur/Maus) - für 24/7-Dauerbetrieb geeignet
- PTZ-Steuerung (z. B. Joystick oder gleichwertig) über VMS-Integration
- Audio-Panel/Lautsprecher für Alarmhinweise; Lautstärke lokal regelbar
- Alle Peripherie-Geräte müssen so positionierbar sein, dass Monitorbilder nicht überdeckt werden

5.4 Mobile Einheiten

- Die mobilen Einheiten müssen über gesicherte Verbindungen (z.B. VPN über 4G/5G/WLAN) mit den KI- und VMS-Servern kommunizieren

- Die mobilen Einheiten sollen über ein Drohnenmodul verfügen mit der Möglichkeit für:
 - o Begrenzung des Aktionsradius durch virtuelle Grenzen (Geofence)
 - o Gesicherte Kommunikation zur Basisstation (wie oben)
 - o Ereignis- oder operatorgesteuerten Start
 - o Programmierung fester Rückkehr- /Abbruchlogiken
- Das Drohnenmodul muss technisch so ausgestattet sein, dass bei Problemen im Flugbetrieb Unfälle vermieden werden. (z.B. Fallschirm, Flugfähigkeit bei Ausfall eines Rotors, redundante Energieversorgung etc.)

6 Nicht-Funktionale Anforderungen (*Punkt 5 der BewM*)

6.1 Verfügbarkeit, Leistung, Redundanz

- Das Gesamtsystem muss eine Gesamtverfügbarkeit von 99,9 % im Monat sicherstellen
- 24/7-Betrieb ohne zwingende Down-Times
- Redundante Systeme und Failover-Mechanismen müssen Datenverluste verhindern
- Eine Betriebswiederherstellung darf nach einem Systemausfall nicht länger als 2 Minuten dauern
- Der Ausfall von Kamera-Live-Bildern ist im VMS dem Operator zu melden, eine Reaktivierung nach Wiederverfügbarkeit muss automatisch erfolgen
- Es muss eine unterbrechungsfreie Stromversorgung für mindestens eine Stunde sichergestellt werden.
- Das VMS soll in der Lage sein, Live-Video mit minimaler Verzögerung von unter 1 Sekunde bereitzustellen.
- Ein Alarm-Ereignis (Echtzeit) soll spätestens nach 4 Sekunden mit den geforderten Parametern (*siehe 4.2.2 - VMS-Live-Betrieb - Verhalten bei Detektion / Alarm*) im VMS angezeigt werden

6.2 Skalierbarkeit

In der Pilotphase werden zunächst drei Objekte ausgewählt.

- Das System muss vertikal und horizontal skalierbar sein
- Erweiterungen (neue Kameras, Module, Zonen, mobile Knoten) können ohne Betriebsunterbrechung integriert werden.

6.3 Exporte / Schnittstellen

- Zur Kopplung mit der Leitstelle muss das System eine offene, dokumentierte API/SDK (Ereignis-Push, Metadaten, Live-Streams, Clip-Abruf) mit Authentifizierung und Protokollierung bereitstellen.
- Ein Kompatibilitätsprofil muss zudem Formate/Protokolle für die konventionelle Aufschaltung (Livebilder, Alarmdaten) benennen.
- Der gesamte Bedien- und Übergabeprozess ist revisionssicher zu protokollieren.
- Das System muss Videoexporte mit dazugehörigen Meta-Daten (Alarmtyp, Kamera, Zeit, Objektklasse) unterstützen und den Export über Time-Lines oder Ereignislisten ermöglichen.
- Es muss eine forensische Exportfunktion unterstützt werden, die Clips mehrerer Kameras synchron inkl. Overlay zusammenführt
- ereignisbezogene Sicherungen werden getrennt gehalten.

6.4 Unterstützte Streaming-Formate / Audio- und Video-Codecs

Von der Leitstelle der Polizei Berlin werden folgende Formate und Codecs unterstützt:

- Streaming-Formate
 - o Apple™ HTTP Live Streaming
 - o Microsoft™ Live Smooth Streaming
 - o Adobe™ Flash HTTP Dynamic Streaming
 - o 3GPP/Edge
 - o RTP + RTCP/UDP
 - o IPTV & PiP: SPTS/UDPProtokolle: FTPS, HTTPS, WebDAV, RTMP, UDP, RTP, RTSP
- Video Codecs:
 - o H.264/MPEG-4 AVC, BP/MP/HP, all levels, up to HD
 - o MPEG-2 MP@ML/HL, up to HD
 - o H.263 Profile 0 Level 45; QCIF or Sub-QCIF
 - o MPEG-4 SP Level 0 to 3, up to CIF
 - o Multi-Bitrate video encoding(MBR)/Adaptive Bit-Rate (ABR)
- Audio Codecs:
 - o MPEG-1 Layer II (SPTS)
 - o MR-NB (RTP)
 - o AAC, LC, HE v1, HE v2, in ADTS or LOAS/LATM

Datensicherheit / Datenintegrität

- Speicher-, Lösch- und Archivvorgaben müssen sich nach dem Konzept zur Archivierung und Löschung von Daten richten;

- Ein rollenbasiertes Berechtigungsmodell muss sicherstellen, dass der Export von Daten oder die Aufhebung von Maskierungen nur von besonders berechtigten Dienstkräften vorgenommen werden können;
- Alle relevanten Bedienhandlungen sind lückenlos zu protokollieren (Login, manuelle Aufschaltungen, PTZ-Steuerungen, Konfigurationsänderungen, Exporte);
- Alle Protokolle führen die AD-Nutzerkennung;
- Datenexporte müssen mit Integritätsnachweis (digital signiert) und gerichtsverwertbar also als unveränderte Rohdaten vorhanden sein. Die Beweiskette (Chain of Custody) ist durchgängig abzubilden.
- Datenexporte in eine Cloud finden nur statt, soweit sie verschlüsselt sind und sich die Systemarchitektur im Einflussbereich der Polizei Berlin befindet.
- Videoaufzeichnungen sind zu verschlüsseln (mindestens AES 256-Bit-Schlüssel)
- Sämtliche Kommunikation zwischen Kamera und KI-Server; KI-Server und VMS-Server muss über sichere und verschlüsselte Verbindungen (behördliches Datennetz oder bei mobilen Einheiten z.B. mittels VPN über 4G/5G/WLAN) erfolgen
- Software, Updates und Patches sind vor Auslieferung vom Hersteller auf Sicherheitslücken und Schwachstellen zu testen

6.5 Logging / Protokolle

- Sämtliche Soft- und Firmware müssen Logfiles mit eindeutigen Meldungen schreiben können
- Jedes System-, Anwendungs- und Benutzerereignis ist in Logfiles zu protokollieren
- Jedes Logfiles soll:
 - o Zeitstempel mit Millisekunden, Herkunft des log-Eintrages und eigentliche Meldung beinhalten und im syslog-Format aufgebaut sein. (Der Hersteller kann eine gleichwertige Alternative zur Bewertung darstellen)
 - o In Loglevel (ERROR, WARN, INFO, ...) kategorisiert werden können
 - o Den Anwendern/Admin eine eindeutige (Fehler-)Meldung liefern
 - o An einer zentralen Stelle in einem gemeinsamen Ordner im Dateisystem abgelegt werden
 - o In der gelieferten Dokumentation inhaltlich und bezüglich des Speicherortes beschrieben werden

6.6 Updates / Change-Management

- Um den sicheren IT-Betrieb der Geräte zu gewährleisten, muss die Software die Möglichkeit für ein browserbasiertes zentrales Update-Management bieten.
- Alle Updates und Patches müssen vom Hersteller im Vorfeld dem AG zusammen mit einem Changelog übermittelt werden
- Backups müssen regelmäßig (Differentialsicherung – täglich, Vollsicherung – wöchentlich) auf einem vom AG genannten Speicherbereich erfolgen

- Die Wiederherstellung auf Basis eines vorher erstellten Backups muss möglich sein
- Bei Updates und Upgrades müssen Nutzer- und Konfigurationsdaten übernommen werden, sie müssen ohne Betriebsunterbrechung durchgeführt werden können
Die Software soll eine Export- und Import-Funktion für Konfigurationsdaten bereitstellen und den Rollback auf eine frühere Version der Konfigurationsdaten unterstützen

6.7 Usability / GUI

- Das VMS muss eine hoch intuitive Benutzeroberfläche bieten, die sowohl für technisch versierte als auch für weniger erfahrene Benutzer leicht verständlich ist.
- Das System muss die geltenden Anforderungen des Landes Berlin zur Software-Ergonomie, Gebrauchstauglichkeit und Barrierefreiheit erfüllen und den Grad der Barrierefreiheit angeben sowie dokumentieren
- Reaktionszeit der Benutzeroberfläche zwischen Klick und Systemaktion < 1 Sekunde.
- Die Software soll unter Hinweisanzeigen adäquat auf Fehleingaben und -bedienungen reagieren bzw. diese im Vorfeld verhindern
- Die Grafikdarstellung darf nicht auf eine einzelne Bildschirmauflösung optimiert sein, sondern muss variabel sein.
- Dargestellte Inhalte müssen dynamisch auf Bildschirmauflösung und Fenstergröße angepasst werden
- Die GUI der Software soll an die Bedürfnisse/Styleguides des Betreibers anpassbar sein.

6.8 Monitoring

- Soft- und Firmware sollen automatische Systemdiagnose sowie ein fortlaufendes Performance-Monitoring bieten

6.9 Support

- Für Soft- und Hardware ist ein deutschsprachiger (min. B2-Niveau des europäischen Referenzrahmens) 24/7 erreichbarer Support sicherzustellen
- Die garantierte Reaktionszeit für den Support bei Problemen mit der Software soll nicht mehr als 1 Stunde betragen
- Die garantierte Reaktionszeit für den Support bei Problemen mit der Hardware soll nicht mehr als einen Werktag betragen
- Reaktionszeit bedeutet, es wird aktiv an der Behebung des Problems gearbeitet, nicht die Entgegennahme der Störungsmeldung
- Die Software soll die Nutzer über eine Nichtverfügbarkeit informieren (Info-Seite mit Wartungshinweis)

7 Schulungen (A)

- Der Auftragnehmer muss Erstbeschulungen für insgesamt ca. 50 Personen (Anwender, Multiplikatoren und Systemadministratoren) der Fachdienststellen hinsichtlich der Bedienung der Systeme und der Möglichkeiten der eingesetzten Software, anbieten.
- Die Schulungen müssen zeitnah vor Beginn des Testbetriebes erfolgen. Genaue Schulungstermine sind mit dem Auftraggeber direkt nach Erteilung des Zuschlags abzustimmen.
- Die Schulungen finden am Sitz des AG statt.
- Die Schulung soll über die Erstschulung in Präsenz hinaus dem Auftraggeber als Videodatei inkl. Audio zur internen Nutzung zur Verfügung gestellt werden.
- zusätzlich ist eine Schulung speziell für die barrierefreie Nutzung aller angebotenen Softwareprodukte zur Verwendung von Eingabehilfen anzubieten.
- Der Anbieter soll ergänzende Online-Schulungsmodule (Training on Demand):
 - Videoschulungen zu Kernfunktionen
 - Differenziert nach Benutzerrolle
 - Jederzeit abrufbarund einen Quick-Guide:
 - Kurzanleitung
 - Übersicht der wichtigsten Funktionen und Bedienelemente
 - Digital und druckbar in deutscher Sprachebereitstellen.
- Bei relevanten Updates oder Funktionsänderungen/-anpassungen sollen für Anwender Auffrischungsbeschulungen angeboten werden. Multiplikatoren und Administratoren müssen über die Änderungen in geeigneter Form informiert werden.

7.1 Anforderungen an Schulungen

Folgende Anforderungen hat der Auftragnehmer für die von ihm durchzuführenden Schulungen zu berücksichtigen:

- Die Trainer verfügen über umfangreiche Praxiserfahrung.
- Die Schulung erfolgt in deutscher Sprache.
- Pro Schulung ist eine Dauer von maximal 1 Tag nicht zu überschreiten
- Auftragnehmer und Auftraggeber stimmen sich in der Vorbereitung und Durchführung der jeweiligen Schulung ab.

Für die Multiplikatoren und Systemadministratoren muss im Nachgang einer Schulung ein telefonischer Support über die Vertragslaufzeit zur Verfügung stehen.

7.2 Anforderungen an Schulungsunterlagen

Folgende Anforderungen hat der Auftragnehmer für die Schulungsunterlagen für die von ihm durchzuführenden Schulungen zu berücksichtigen:

- Die Schulungsunterlagen müssen in deutscher Sprache mindestens zwei Wochen vor Beginn der Schulungen vorliegen.
- Der Auftragnehmer ist verpflichtet, dem Auftraggeber die für die Schulungen erstellten Schulungsunterlagen (Präsentationen, Videos, etc.) zur Verfügung zu stellen. Erforderliche Handbücher, Manuals o.ä. sind jedem Teilnehmer einmal zur Verfügung zu stellen.
- Die Schulungsunterlagen sind als farbige Hardcopy (Papierform) und als elektronisches Medium (barrierefreie, druckfähige PDF-Datei) einmal pro Teilnehmer zur Verfügung zu stellen. Präsentationen sind als PDF-Datei zur Verfügung zu stellen.
- Die Schulungsunterlagen sind dem Auftraggeber spätestens 8 Wochen vor Durchführung der ersten Schulung zur Durchsicht zu übergeben und mit diesem abzustimmen.

7.3 Schulung Anwender/Multiplikatoren

Der Auftraggeber sieht vor, 40 Mitarbeitende der Polizei Berlin durch den Auftragnehmer in der Bedienung und Nutzung der Software-Lösung auszubilden. Diese Mitarbeitenden sollen im Anschluss das System als Anwender bedienen können.

Die Schulung für Anwender muss aus einer Grundschulung und einer Praxisschulung bestehen. Die Grundschulung muss beim Auftraggeber erfolgen. Die Grundschulung muss theoretische Kenntnisse vermitteln, insbesondere:

- Systemübersicht
- Leistungsmerkmale und deren Nutzung
- Software-Beschreibung
- Aufbau
- Technische Beschreibung
- Technische Daten

Die weiterführenden Praxisschulungen müssen insbesondere folgende Inhalte vermitteln:

- Bedienung der Module (Software, Hardware)
- Systeme am Arbeitsplatz
- Bedienoberflächen (GUI)
- Nutzung / Konfiguration der Barrierefreiheit in der Videomanagement-Software
- Zusammenhänge zwischen den Modulen der Anwendung

Die Schulung muss so aufgebaut sein, dass die beschulten Mitarbeiter befähigt werden, als Multiplikatoren weitere zukünftige Anwender selbstständig zu beschulen.

7.4 Schulung Systemadministratoren

Der Auftraggeber sieht vor, 10 Mitarbeitende der Polizei Berlin in der Administration und der Anwendung des Systems d.h. für alle HW-/SW-Komponenten des zu liefernden Systems auszubilden, so dass diese später das System administrieren können.

Durch den Auftragnehmer kann dabei vorausgesetzt werden, dass der zu schulende Personenkreis über Grundkenntnisse und Erfahrung mit modernen IT-Systemen besitzt. Die Schulung muss aus einer Grundschulung und einer Praxisschulung bestehen. Die Grundschulung muss beim Auftraggeber erfolgen. Die Grundschulung muss theoretischen Kenntnisse vermitteln, insbesondere:

- Übersicht über die Systeme
- Leistungsmerkmale und deren Nutzung
- Software-Beschreibung
- Aufbau
- Technische Beschreibung
- Technische Daten

Die Praxisschulung muss beim Auftraggeber in Berlin erfolgen. Die weiterführenden Praxisschulungen müssen insbesondere folgende Inhalte vermitteln:

7.4.1 Bedienung der Module (Software, Hardware)

- Sicherheitsbestimmungen
- Aufbau
- Inbetriebnahme / Außerbetriebnahme
- Bedienung, Steuerungs- und Überwachungsmöglichkeiten
- Betrieb bei Störungen und Wiederherstellung des ungestörten Betriebes

7.4.2 Wartung und Instandsetzung

- Sicherheitsbestimmungen
- Wartungsarbeiten
- Instandsetzungsarbeiten

7.4.3 Zusätzliche Inhalte angepasst auf Ebene des 2nd-Level-Supports:

- System-/Gerätebeschreibung aus Sicht eines Administrators
- Installation und Basiskonfiguration
- Administration und Konfiguration

- Netzwerk- und Firewall-Administration
- Platten- und Datenträger-Administration
- Dateisysteme
- Nutzer und Gruppen
- Rollen und Rechte
- Dienste
- Protokollierung
- Pflege und Änderung von Zugriffsrechten
- Backup und Restore
- Versionspflege (Update von Software)
- Pflege von Datenbanken
- Fehlersuche, Austausch von Schadgeräten, Konfiguration von Ersatzgeräten
- Fehlersuche

8 Konzepte

In Abstimmung mit dem Auftraggeber sind die in Anhang 6 dargestellten Konzepte durch den Auftragnehmer zu erstellen. Hierfür ist ein kalkulatorischer Preis pro Personentag anzugeben. Die Konzepte müssen die in dieser Leistungsbeschreibung benannte Umgebung und den Stand der Technik berücksichtigen.

9 SLA - Service Level Agreements

Siehe EVB-IT-System-Vertrag.

10 Richtlinien zur Systemtechnik

Ab 2025 ist die Polizei Berlin gesetzlich verpflichtet den Netzbetrieb gemäß IPv6 durchzuführen.

Die Polizei Berlin behält sich vor, bei Bedarf eine Hardware-Plattform / Infrastruktur im Rechenzentrum zur Verfügung zu stellen. Die Anforderungen und Details sind im Anhang 4 „Richtlinien zu Systemtechnik und Transportnetz“ zu finden.

10.1 LAN-Security 802.1x (Authentication)

Siehe Anhang 4 „Richtlinien zu Systemtechnik und Transportnetz“.

10.2 IPv6

Siehe Anhang 4 „Richtlinien zu Systemtechnik und Transportnetz“.

11 Lizenzen (A)

Im Rahmen der Softwarelizenzen, muss der Hersteller detaillierte Angaben zu folgenden Aspekten machen:

11.1 Lizenzbedingungen

- Nutzungsrechte (Umfang und Einschränkungen)
- Verbreitungsrechte
- Modifikationsrechte
- Weitergaberechte

11.2 Lizenzlaufzeit

- Dauer der Lizenz (zeitlich begrenzt oder unbefristet)
- Verlängerungsbedingungen
- Kündigungsbedingungen

11.3 Anzahl der Lizenzen

- Anzahl der Benutzerlizenzen (Single-User, Multi-User)
- Anzahl der Installationen (Einzelninstallation, Mehrfachinstallation)

11.4 Rechts- und Haftungsfragen

- Haftungsausschlüsse
- Gewährleistungen
- Rechtliche Konsequenzen bei Lizenzverletzungen

11.5 Sicherheits- und Datenschutzanforderungen

- Anforderungen an Datenschutz und Datensicherheit
- Konformität mit gesetzlichen Vorgaben (z.B. DSGVO)

11.6 Einschränkungen und Sonderbedingungen

- Nutzungseinschränkungen (z.B. geografische Beschränkungen)
- Besondere Bedingungen für bestimmte Anwendungsfälle

11.7 Migration und Interoperabilität

- Bedingungen für die Migration von bestehenden Systemen
- Bedingungen für die Migration in eine externe Cloudlösung
- Interoperabilität mit anderen Systemen und Softwarelösungen

11.8 Lizenzmanagement

- Verfahren zur Lizenzverwaltung und -überwachung
- Berichtspflichten und Audits

12 Anhänge

Anhang 1 - Vertraulichkeitserklärung

Anhang 2 - Ausschlusskriterien Barrierefreiheit

Anhang 3 - IKT Architekturrichtlinie Land Berlin 2.0

Anhang 4 - Richtlinien Systemtechnik und Transportnetze

Anhang 5 - Konzepte

Anhang 6 - Schutz- und Beobachtungsbereiche

Die Anhänge 3-4 sowie das Fachkonzept zu dem Projekt werden erst nach Vorlage der Vertraulichkeitserklärung zusammen mit der Aufforderung zur Abgabe eines Angebotes zur Verfügung gestellt.