

## **Nutzerrollen**

Besucher:

Externe Gäste, Lieferanten, Partner und weitere Besucher benötigen ein möglichst einfaches, mobiles Voranmelde- und Check-in-Verfahren im BMS. Das BMS muss dabei QR-Code-basiert sein und beim Anmelden sowie Check-in klare Anweisungen zu Sicherheitsregeln und Parkmöglichkeiten geben.

Unternehmensmitarbeitende / Einlader:

Diese Nutzer können Besucher anmelden. Das BMS muss hierfür ein unkompliziertes Web-Formular mit integrierten Erinnerungsfunktionen, Bearbeitungsmöglichkeiten und Nachverfolgbarkeit von Einladungen bereitstellen.

Sicherheitsdienst / Facility Management:

Dies sind operative Nutzer, die die Einlasskontrolle und Überwachung durchführen. Das BMS muss für diese Nutzer ein Echtzeit-Dashboard, Filtermöglichkeiten, Alarmregeln, eine schnelle Suche aller Nutzer und so wenige manuelle Prüfungen wie möglich bieten. Zudem muss das BMS diesen Nutzern die Möglichkeit geben, vor Ort neue Gäste spontan registrieren zu können.

Administratoren und IT-Team:

Die Administratoren und das IT-Team sind verantwortlich für Betrieb, Rechteverwaltung (Rollenverteilung), Reporting sowie Integration von Erweiterungen und Fehlerbehebungen. Das BMS muss diese Nutzer in der zentralen Administration unterstützen, eine SSO-Integration bieten und eine klare Betriebsdokumentation ermöglichen.

## **Einsatzumgebung**

Das BMS muss als webbasiertes System entwickelt werden, das in aktuellen Browsern sowohl auf mobilen Endgeräten als auch auf PCs nutzbar ist und über ein responsives Design verfügt.

Zudem wird das Besuchermanagementsystem (BMS) auf der vorhandenen IT-Infrastruktur der TechPort Berlin GmbH On-Premise entwickelt. Dabei verfügt das BMS über die Möglichkeit einer containerisierten Bereitstellung, die mithilfe von Docker und Kubernetes umgesetzt wird.

Der Betrieb erfolgt über das LAN- und WLAN-Netzwerk des Campus. Zudem ist das System in das bestehende Intranet-Portal integriert und verfügt über Schnittstellen zu den vorhandenen Zutrittskontrollsystmen, die über definierte APIs angebunden sind.

## Funktionale Anforderungen

F01 Voranmeldung durch Mitarbeitende:

Die Voranmeldung erfolgt über ein strukturiertes Web-Formular, in das Mitarbeitende alle relevanten Besucherdaten eintragen. Alternativ hätte die Anmeldung per E-Mail erfolgen können, was jedoch zu unvollständigen Informationen und einem erhöhten manuellen Bearbeitungsaufwand geführt hätte. Auch eine telefonische Anmeldung wäre möglich gewesen, jedoch fehlt hierbei eine automatische Dokumentation und Nachvollziehbarkeit. Das Web-Formular stellt sicher, dass alle erforderlichen Daten standardisiert erfasst werden und sofort im System verfügbar sind. Daher wurde diese Lösung gewählt, um Prozesse effizienter und weniger fehleranfällig zu gestalten.

#### F02 Bestätigungen & QR-Codes:

Für den Check-in wurde eine QR-Code-basierte Lösung gewählt, bei der Besucher nach der Anmeldung automatisch einen Code erhalten, der beim Betreten des Geländes gescannt wird. Eine mögliche Alternative wäre die manuelle Anmeldung durch den Sicherheitsdienst gewesen, bei der Besucher ihren Namen nennen und im System gesucht werden. Diese Lösung hätte jedoch zu längeren Wartezeiten und einer höheren Fehleranfälligkeit geführt. Eine weitere Alternative wäre der Einsatz von RFID-Karten gewesen, die Besucher beim Eintritt scannen. Dies hätte jedoch zusätzliche Hardware sowie einen erhöhten Verwaltungsaufwand verursacht. Die QR-Code-Lösung wurde gewählt, da sie kosteneffizient ist, schnell funktioniert und keine zusätzliche Infrastruktur benötigt.

#### F03 Erinnerungs- und Änderungsfunktion:

Das BMS versendet automatisierte Erinnerungs-E-Mails 24 h und 2 h vor dem Termin. Zusätzlich erhält der Einlader die Möglichkeit, Termine zu ändern oder zu stornieren. Den Besuchern werden ebenfalls Möglichkeiten geboten, Termine zu stornieren oder optional zu ändern. Alle Änderungen werden im Audit-Trail versioniert gespeichert.

#### F04 Bulk-/CSV-Import:

Für Veranstaltungen und Workshops stellt das System eine Bulk-Upload-Funktion im CSV-Format zur Verfügung, mit der mehrere Besuchereinträge gleichzeitig angelegt werden können; einschließlich eines Validierungsfehler-Reportings.

#### F05 Check-in via QR-Code:

Besucher zeigen am Empfang oder am Terminal ihren QR-Code vor. Das System validiert diesen QR-Code und ändert den Status automatisch zu „eingecheckt“, welcher dann im Dashboard in Echtzeit sichtbar ist.

#### F06 Walk-in-Erfassung:

Der Sicherheitsdienst kann Walk-in-Besucher über ein vereinfachtes Terminalformular erfassen; das System erzeugt einen temporären Eintrag, fordert bei Bedarf eine Identitätsprüfung an und markiert solche Einträge als „Walk-in“.

#### F07 Optionale Identitätsprüfung mit OCR:

Ausweise können optional per OCR ausgelesen werden. Dieser Prozess wird nur nach DSGVO-Prüfung und vorhandener gesetzlicher Rechtsgrundlage aktiviert. Die Speicherung erfolgt ausschließlich gemäß der konfigurierten Retention-Policy.

#### F08 Besucherausweise & Kurzzeit-PINs:

Das BMS kann digitale und druckbare Besucherausweise sowie zeitlich befristete PINs erzeugen, mit denen sich Besucher ebenfalls einchecken können. Die Besucherausweise verfügen über einen festgelegten Gültigkeitszeitraum.

#### F09 Echtzeit-Dashboard für Sicherheitsdienst:

Das Dashboard zeigt aktuell eingeloggte Besucher, erwartete Ankünfte, Walk-ins und Fahrzeugkennzeichen an. Im Dashboard kann nach Unternehmen, Zeitfenster und Bereichen gefiltert werden. Zudem sind Exportfunktionen vorhanden.

#### F10 Konfigurierbare Warnregeln und Eskalationen:

Administratoren und Sicherheitsmitarbeitende können Regeln und Sicherheitswarnungen konfigurieren (z. B. begrenzte Anzahl an Walk-ins, eingeschränkte Parkmöglichkeiten bei unbekannten Kennzeichen, Einträge auf Sperrlisten). Diese Regeln lösen automatische Benachrichtigungen per E-Mail, SMS und Dashboard-Popups aus.

#### F11 Audit-Trail & Protokollierung:

Anmeldungen, Änderungen, Check-ins, Check-outs und Administrator-Aktionen werden mit Nutzer-ID, Zeitstempel, IP und Änderungsdetails append-only protokolliert. Audit-Logs sind exportierbar und werden gemäß Retention-Policy vorgehalten.

#### F12 Standard-Reporting & Export:

Das BMS erstellt Besucherstatistiken, ermittelt Spitzenzeiten, berechnet Voranmeldequoten und durchschnittliche Wartezeiten und bietet eine Exportmöglichkeit in CSV und PDF. Nutzer können die zeitliche Aggregation (z. B. täglich, wöchentlich, monatlich) auswählen.

#### F13 Rollenbasierte Zugriffskontrolle (RBAC):

Für den Systemzugriff wurde eine rollenbasierte Zugriffskontrolle implementiert, bei der Nutzer abhängig von ihrer Rolle bestimmte Berechtigungen erhalten. Eine Alternative wäre gewesen, allen Nutzern die gleichen Rechte zu vergeben, was jedoch ein erhebliches Sicherheitsrisiko dargestellt hätte. Ebenso hätte man individuelle Berechtigungen für jeden Nutzer manuell festlegen können, was jedoch sehr verwaltungsaufwendig und fehleranfällig wäre. RBAC bietet hingegen eine klare Struktur, erhöht die Datensicherheit und lässt sich auch bei steigender Nutzerzahl effizient verwalten. Aus diesen Gründen stellt diese Methode den etablierten Standard für professionelle Informationssysteme dar.

#### F14 Mandanten-/Bereichskonfiguration:

Es wird die Möglichkeit geboten, mehrere Campus-Bereiche oder Mandanten mit individuellen Einstellungen (z. B. Empfangszeiten, Pflichtfelder oder Workflows) zu verwalten, ohne dass Codeänderungen erforderlich sind.

#### F15 Konfigurierbare Formulare und Workflows:

Administratoren können Pflichtfelder, Erinnerungsintervalle, Check-in-Methoden und Timer konfigurieren, sodass das System bereichsspezifisch angepasst werden kann.

#### F16 Single-Sign-On / Identity Provider:

Das System unterstützt SAML 2.0 oder OAuth2/OpenID Connect zur Integration mit dem TechPort Identity Provider für Mitarbeitenden-Anmeldung und rollenbasierte Rechtevergabe.

#### F17 API für Intranet & Drittsysteme:

Das BMS stellt eine RESTful API (OpenAPI/Swagger-Spec) für Voranmeldung, Statusabfrage und Reporting bereit; die Authentifizierung erfolgt über OAuth2.

#### F18 Schnittstelle zu Zutrittssystemen:

Für die Übergabe von Freigabeereignissen an Schranken und Drehkreuze werden Event-APIs/Webhooks verwendet. Das Empfangen von Zustandsmeldungen ist mit der Hardware möglich; dies muss jedoch technisch definiert werden.

#### F19 Benachrichtigungssystem & Fallback:

SMTP wird für E-Mails integriert; ein optionales SMS-Gateway kann angebunden werden. Ein Fallback-Mechanismus muss definiert werden, damit kritische Benachrichtigungen bei Ausfall eines Providers dennoch zugestellt werden können.

#### NF1 Performance:

Alle Seiten und kritischen Funktionen müssen im 90. Perzentil eine Ladezeit von unter 2 Sekunden erreichen, bei einem Lastszenario mit bis zu 500 gleichzeitigen Nutzern. Die Messung erfolgt durch Lasttests mit k6, wobei Perzentilwerte ermittelt und dokumentiert werden.

#### NF2 Skalierbarkeit:

Die Systemarchitektur erlaubt eine horizontale Skalierung (z. B. Containerisierung mit Auto-Scaling) und ist bei Bedarf auf bis zu 2.000 gleichzeitige Nutzer erweiterbar, ohne dass Änderungen am Datenbankmodell erforderlich sind.

#### NF3 Verfügbarkeit & SLA:

Das Betriebsmodell stellt eine Verfügbarkeit von mindestens 98 % pro Monat sicher. Geplante Wartungsfenster werden vorab angekündigt. Ungeplante Ausfälle werden gemessen, dokumentiert und ausgewertet.

#### NF4 Backup, RTO und RPO:

Das System erstellt täglich verschlüsselte Backups, die eine zuverlässige Wiederherstellung des Betriebs gewährleisten. Die maximale Wiederherstellungszeit (RTO) beträgt höchstens 4 Stunden, während der maximal zulässige Datenverlust (RPO) auf 24 Stunden begrenzt ist. Zusätzlich werden regelmäßige Wiederherstellungstests (Restore-Tests) durchgeführt und dokumentiert, um die Funktionsfähigkeit der Backups sicherzustellen.

#### NF5 Datenübertragung:

Alle Datenübertragungen erfolgen über TLS 1.2 oder höher. Sensible Daten werden im Ruhezustand verschlüsselt gespeichert. Die TLS-Konfiguration entspricht den aktuellen Best Practices.

#### NF6 Zugriffskontrolle & Zwei-Faktor-Authentifizierung:

Eine rollenbasierte Zugriffskontrolle (RBAC) ist für das BMS verpflichtend. Administrative Zugriffe erfordern zusätzliche Schutzmaßnahmen wie Zwei-Faktor-Authentifizierung (2FA) sowie eine umfassende Auditierung.

#### NF7 DSGVO & Datenschutz:

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich auf einer gültigen Rechtsgrundlage. Einwilligungen werden dokumentiert, und Besucherdaten werden nach 24 Monaten gelöscht. Mit allen relevanten Drittanbietern werden Auftragsverarbeitungsverträge (AV-Verträge) abgeschlossen.

#### NF8 Audit & Logging:

Audit-Logs sind append-only, werden mindestens ein Jahr aufbewahrt und sind konfigurierbar. Die Logs sind für forensische Analysen sowie für Abnahmezwecke exportierbar.

#### NF9 Usability & Schulungsaufwand:

Die Benutzeroberfläche ist intuitiv, barrierearm und – soweit möglich – WCAG 2.1 AA-konform gestaltet. Der Sicherheitsdienst sowie Mitarbeitende sollen die Kernfunktionen innerhalb von einem Arbeitstag erlernen und sicher bedienen können.

## NF10 Wartbarkeit & Testabdeckung:

Die Codebasis wird mit technischer Dokumentation, Deployment-Anleitungen sowie einer empfohlenen Testabdeckung von mindestens 80 % durch Unit-Tests für kritische Module ausgeliefert. Minor-Updates müssen ohne längere Downtimes deploybar sein.

## Schnittstellen & Integration

### Intranet\_Portal:

Ein OAuth2-gesichertes REST-API wird bereitgestellt, sodass das bestehende Intranet den Besucherstatus lesen kann.

### Identity Provider:

SAML2 oder OpenID Connect wird zur Authentifizierung der Mitarbeitenden genutzt. Nutzerattribute werden bei der ersten Anmeldung übernommen.

### Zutrittssysteme:

Webhooks werden für die Übergabe von Freigaben an Schranken mit Rückmeldung über Geräteteststatus genutzt. Protokoll und Authentifizierungsdetails werden technisch überprüft.

### Benachrichtigungsdienste:

SMTP-Server werden für Standard-Mails genutzt, optional werden SMS-Provider mit Fallback funktion bereitgestellt. Alle externen Provider benötigen hierbei einen AV-Vertrag.

### Monitoring & Logging:

Schnittstellen zu Monitoring-Tools und SIEM für Security-Events werden definiert.

### Oberfläche / UX

**Terminal UI für Empfang/Security:** Ein vereinfachtes, tablet-taugliches Terminal mit großen Schaltflächen, schneller Suchfunktion, QR-Scanner-Unterstützung und einer Notfalltaste wird angefertigt.

**Responsive Voranmeldeformular:** Besucher-Formular ist selbsterklärend, zeigt nur notwendige Pflichtfelder und bietet Inline-Validierung. Mehrsprachigkeit (DE/EN) wird initial unterstützt.

**Dashboard-Visualisierung:** Farbliche Kennzeichnung von vorangemeldeten vs. Walk-in-Besuchern, Filterbarkeit nach Unternehmen und Bereich sowie Export-Buttons sind vorhanden.

## Datenmodell & Datenschutzdetails

Datenkategorien: Stammdaten (Name, Firma, E-Mail), Besuchsmetadaten (Datum, Dauer, Ansprechpartner), optionale Sicherheitsdaten (Kennzeichen, Ausweisfoto) sowie Systemdaten (Audit).

Retention & Löschkonzept: Standard-Retention für Besucherdaten: 24 Monate. Audit-Logs: mindestens 12 Monate, Löschverfahren inklusive Archivierung/Anonymisierung werden definiert und DSGVO-konform umgesetzt.

Einwilligung / Rechtsgrundlage: Besucher erhalten bei Check-in eine Informationsanzeige zur Verarbeitung; für optionale Foto-/OCR-Verarbeitung wird eine explizite Einwilligung eingeholt und protokolliert.

AV-Verträge & Hosting: Falls externe Provider (E-Mail, SMS, Cloud) genutzt werden, sind schriftliche Auftragsverarbeitungsverträge (AVV) abzuschließen.

## Systemarchitektur und Betriebskonzept

Architekturrempfehlung: Containerisierte Microservice-Architektur (Docker/Kubernetes), Load-Balancer, relationale DB (PostgreSQL), Redis für Caching, Prometheus/Grafana für Monitoring. CI/CD-Pipeline (GitHub Actions) mit Staging und Produktion.

Betriebsverantwortung: TechPort IT übernimmt Betrieb und Rechteverwaltung. Durch Dienstleister erbrachte Entwicklung kann mit SLA für Support ergänzt werden.

Backup & Restore: Vollständige tägliche Backups und regelmäßige Restore-Tests werden dokumentiert. Notfall-Runbook enthält Schritte für RTO ≤ 4 Stunden.

## Tests, Abnahme & Metriken

Testarten: Unit-Tests, Integrationstests, End-to-End Tests ( Playwright), Performance-Tests (k6), Penetrationstest durch externen Dienstleister.

Abnahmekriterien:

A1: Durchschnittliche Wartezeit an Zufahrten reduziert um ≥ 30.

A2: Voranmeldequote ≥ 60 % innerhalb 6 Monate nach Go-Live.

A3: Reduktion manueller Prüfungen ≥ 50 %.

A4: 90. Perzentil der Seitenladezeit ≤ 2s bei 500 gleichzeitigen Nutzern.

A5: Verfügbarkeit ≥ 98 % pro Monat.

A6: Penetrationstest ohne kritische Sicherheitslücken.

Akzeptanzprozess: Für jede Abnahmeanforderung wird ein Testfall mit erwartetem Ergebnis und Testdaten definiert. Abnahme erfolgt nach erfolgreich bestandenen Tests und formaler Freigabe durch Auftraggeber.

#### Liefergegenstände

Produktionsbereite Web-Applikation mit Source-Code und Deployment-Scripts.

OpenAPI/Swagger-Spezifikation für alle bereitgestellten APIs.

Benutzerhandbuch, Administratorhandbuch, Integrationsdokumentation und Betriebshandbuch.

Schulungsunterlagen: kurze Videotutorials für Empfang/Security/Mitarbeiter + Präsentationsfolien für Einführung.

Test- und Abnahmeberichte und Abnahmeprotokoll.

#### Zeitplan, Budget und Meilenliste

Budgetrahmen: 150.000 – 250.000

Projektlaufzeit: 1 Jahr (Meilensteine) : Kickoff (Woche 0) → Anforderungs-Review (W4) → Prototyp Voranmeldung + Check-in (W12) → Integration SSO + Intranet (W20) → Feature-Complete (W36) → Tests & Security-Audit (W40–44) → Pilotbetrieb (W46) → Go-Live & Wissenstransfer (W52).

Budgetaufteilung: Analyse 10 %, Entwicklung 60 %, Infrastruktur 10 %, Tests & Abnahme 10 %, Schulung & Dokumentation 10 %.

#### Support, Wartung & SLA-Vorschlag

SLA-Modelle: Bronze (48 h Reaktionszeit), Silber (24 h), Gold (4 h) — Leistungen und Kosten sind vertraglich zu regeln.

Wartungsplan: Regelmäßige Security-Patches, monatliche Backup-Prüfungen, halbjährliche Restore-Tests und jährliche Penetrationstests.

#### **Risiken & offene Punkte (mit Milderungsmaßnahmen)**

**On-Prem vs. Cloud-Entscheidung:** Risiko: Auswirkungen auf RTO/RPO und Kosten.  
Maßnahme: Entscheidung basierend auf Compliance & TCO-Analyse, Proof-of-Concept für beide Optionen.

**Schnittstellen zum Zutrittssystem unklar:** Risiko: Verzögerungen bei Integration.  
Maßnahme: Frühzeitige technische Abfrage des Herstellers, Prototyp-Test mit simuliertem Interface.

**DSGVO-Unsicherheiten bei Ausweisfotos:** Risiko: rechtliche Probleme. Maßnahme: Rechtsprüfung, klare Einwilligungs-UI und minimale Speicherung/Anonymisierung.

**Benutzerakzeptanz (Mitarbeitende/Besucher):** Risiko: geringe Voranmeldequote.  
Maßnahme: einfache UX, Erinnerungskampagnen, kurze Schulungen und Pilot mit Feedbackschleifen.

**Performance unter Stoßlast:** Risiko: langsame Ladezeiten. Maßnahme: Lasttests in mehreren Szenarien, Caching-Strategie und horizontale Skalierung.

**Provider-Ausfall (E-Mail/SMS):** Risiko: Benachrichtigungsversagen. Maßnahme: Fallback-Provider und Queueing-System für Nachrichten.

Glossar:

**Walk-in-Besucher:** Besucher ohne vorherige Anmeldung.

**Audit-Trail:** Unveränderliche Protokollierung aller relevanten Aktionen.

**RTO / RPO:** Recovery Time Objective / Recovery Point Objective — Wiederherstellungs- und Datenverlustziele.

**RBAC:** Role-Based Access Control.

**SSO:** Single Sign-On (SAML2, OpenID Connect).