Visitor Management System
Standardization Check List

Deployed globally, centralized Visitor Management System (VMS) has to satisfy the needs related to different geographies, address different security and compliance requirements, fit variety of visitor type requirements, and enable use cases of global enterprise-grade facilities.

SCALABILITY

- ✓ Manage multiple locations (lobbies, events, gates)
- ✓ Control access with User roles
- ✓ User roles

CUSTOMIZATION

- Visitor types ✓
- Localization ✓
- Branding ✓

SECURITY

- ✓ SOC 2
- ✓ Data residency
- ✓ Single tenant

INTEGRATION

- Build custom integrations with other business systems ✓
- Laverage data ✓

Leverage the checklist below to evaluate solutions against scalability, customization, security, and integration considerations that will enable Visitor Management initiative to scale now and support your future growth.

Standardization Check List

Scalability

The solution should be possible to configure to location, business unit and office geography.	✓
The system should provide multiple custom permission bundles for different types of users available.	✓
The system should allow to immediately deploy new locations or user experiences.	✓
The system should recognize repeat visitors and track document signature status and expiries.	✓
System should recognize repeat visitors across different locations and auto-fill details, recognizing previously signed documents.	✓

Customization

System should provide custom workflows and user-specified triggers.	✓
The system should provide custom branding for locations, subsidiaries and location types.	✓
Different languages should be enabled for different locations or users.	✓
System should allow visitors to be classified into different user types.	✓
System should include management of processes beyond the lobby (eg. Guard gates, parking, pre-registration).	✓
System should allow for custom badge layouts, variety of badge materials and expiry mechanisms.	✓
System should allow for signature of multiple document types.	✓
System should allow for removal of all vendor branding and advertising.	✓

Security

Solution provider should have enterprise security certifications, such as SOC2	✓
Platform deployment should be available in regional data centers	✓
Local data residency option should be available	✓
Single tenant deployment option should be available	✓
Centralized global watchlists should be managed across different locations	✓
Watchlist should allow for at minimum 3 custom list definitions and uniquely configured workflows	✓
System should provide Government ID and passport validation by enterprise-grade scanners	✓
System should comply with all US and International privacy regulations, such as GDPR	✓
System should comply with applicable industry regulations (ITAR, PCI, FISMA, GMP etc.)	✓
Solution should provide a real time view of who is on site at any given time	✓

Integration

System should provide integrations with Single Sign On technologies such as SAML 2.0, Active Directory, etc.	✓
System should enable integrations with business productivity platforms such as outlook	✓
System should enable custom integrations via Rest API	✓