



FACIAL RECOGNITION (FR) SOFTWARE

Technical Specifications & Data Sheet

1. Product Overview & Deployment

Parameter	Specification / Requirement	Remarks / Acceptance Criteria
Product Type	AI-based Facial Recognition software for live CCTV feeds, recorded video and image-based face matching.	Suitable for surveillance, attendance, access control, visitor management and watchlist monitoring.
Deployment Model	On-premises, private cloud or hybrid deployment.	Final model to be confirmed as per client IT, security and network policy.
Supported Recognition Modes	1:N identification against enrolled database/watchlists and 1:1 verification for identity validation.	Both modes shall be configurable based on use case.
User Interface	Web-based dashboard for live monitoring, enrolment, watchlist management, alerts, reports and administration.	Accessible only to authorised users.
Multi-Site Operation	Supports centralised monitoring of multiple locations/camera groups subject to network and architecture design.	Site, location and camera mapping shall be configurable.

2. Core Functional Specifications

Parameter	Specification / Requirement	Remarks / Acceptance Criteria
Face Detection	Automatically detects human faces from live video streams, recorded footage and uploaded images.	Detection quality depends on camera angle, lighting, face size and visibility.
Face Recognition	Extracts facial features and matches detected faces against enrolled persons, authorised lists or watchlists.	Output shall include person details, confidence score, camera name, location and timestamp.
Face Enrolment	Supports manual enrolment, live camera capture and bulk import of face images with metadata.	Fields may include name, ID, category, department, validity period, remarks and watchlist mapping.
Watchlist Management	Multiple watchlists such as blacklist, VIP, staff, visitor, contractor, suspect and restricted-entry list can be created and maintained.	A person may be assigned to one or more categories as per workflow.
Unknown Face Logging	Unrecognised faces can be captured and stored as unknown face events for review and investigation.	Storage and retention to be configured as per client policy.
Duplicate Enrolment Check	System shall assist in identifying duplicate or similar face records during enrolment.	Configurable threshold preferred.
Face Quality Check	System shall support quality validation for blur, insufficient lighting, face angle and low face visibility.	Poor-quality images shall be flagged before enrolment where applicable.



3. Camera, Input & Configuration

Parameter	Specification / Requirement	Remarks / Acceptance Criteria
Video Input	RTSP stream, ONVIF-supported camera stream, VMS stream, NVR feed or recorded video input, subject to device/API availability.	Integration shall depend on stream accessibility and credentials.
Supported Media Formats	Common camera streams using H.264/H.265 and image formats such as JPG, JPEG and PNG.	Codec support may vary depending on source device/VMS.
Recommended Camera Placement	Entry/exit gates, corridors, reception areas, access points, choke points and other locations with clear frontal face view.	Camera shall preferably capture frontal or near-frontal faces.
Image Quality Conditions	Adequate lighting, minimal backlight, low motion blur and sufficient face size in frame are required for reliable recognition.	Helmets, masks, scarves, caps and reflective glasses may reduce accuracy.
Camera Mapping	Each FR-enabled camera shall be mapped with camera name, location, zone, stream URL and applicable use case.	Configuration shall be editable by authorised administrator.

4. Alerts, Search & Reports

Parameter	Specification / Requirement	Remarks / Acceptance Criteria
Real-Time Alerts	Generates alerts for watchlist match, blacklist match, unauthorised detection, unknown face detection and restricted-area recognition.	Alerts shall show snapshot, person details, confidence score, camera, location and time.
Alert Handling	Alert acknowledgement, filtering, status tracking and historical alert review shall be available.	Active and historical alerts shall be clearly separated.
Person Search	Search person appearance by name/ID, camera, category, location, date, time and confidence score.	Shall support investigation across live and historical events.
Reports	Recognition report, watchlist alert report, unknown face report, attendance report, camera-wise report, user activity log and audit trail.	Export to Excel/CSV/PDF subject to project requirement.
Event Record	Each recognition event shall store timestamp, camera/location, face snapshot, matching result, confidence score and event status.	Retention period shall be configurable.

5. Integration, Security & Compliance

FACIAL RECOGNITION (FR) SOFTWARE

Technical Specifications & Data Sheet



Parameter	Specification / Requirement	Remarks / Acceptance Criteria
Integration Interfaces	REST API/JSON-based integration with VMS, access control, flap barriers, attendance systems, visitor management, command centre and notification gateways.	Third-party integration requires API/SDK/documentation from respective system provider.
Role-Based Access	User roles such as administrator, supervisor, operator and viewer shall control access to modules and data.	Access to enrolment, deletion, export and reports shall be permission-based.
Audit Trail	System shall log user login/logout, configuration changes, enrolment changes, alert actions and report downloads.	Audit logs shall be available for authorised review.
Data Protection	Supports controlled access to face database, configurable data retention, restricted export and secure communication where enabled.	Client shall define privacy, consent and retention policy before deployment.
Backup & Restore	Face database, metadata, configuration and reports shall support backup and restoration as per deployment policy.	Backup frequency to be agreed during implementation.

6. Assumptions & Exclusions

Parameter	Specification / Requirement	Remarks / Acceptance Criteria
Dependencies	Recognition accuracy depends on camera quality, lighting, face angle, distance, occlusion, network stability and enrolled image quality.	Site survey and camera view validation are recommended before final commissioning.

Privacy & Compliance Note: Facial Recognition systems may be subject to local data protection, biometric data and privacy laws. Client is responsible for ensuring lawful deployment, obtaining required consent and defining data retention and access policies prior to commissioning.