



IMPLEMENTATION & OPERATIONS

Facial Attendance System

A guide to what was built, how face-only kiosk attendance works, how it is secured, and how administrators should deploy and test it.

Branch locked

Every authorized kiosk is assigned to one branch.

Privacy first

No raw camera image is uploaded or retained.

Two modes

Employee-ID verification or opt-in face-only identification.

Executive summary

The HRIS now includes an administrator-controlled facial-attendance kiosk on the login page. Administrators define the approved privacy policy, enroll employees, authorize a browser for one branch, and may separately enable face-only identification.

1:1
Employee selects an enrolled branch record; only that template is checked.

1:N
No ID is entered; active templates in the kiosk branch are checked.

0 images
Raw camera frames stored or uploaded by the feature.

Important legal and privacy boundary
Technical safeguards support compliance, but they do not make a deployment lawful by themselves. The organization's DPO or legal/privacy officer must approve the real PIA, lawful basis, notice, necessity and proportionality assessment, fallback, retention, and employee-rights procedures. Face-only 1:N identification must be addressed explicitly.

Guide contents

1. Work completed	3	5. Employee kiosk guide	7
2. How the system works	4	6. Technical reference	8
3. Privacy and security	5	7. Performance and troubleshooting	9
4. Administration guide	6	8. Testing and acceptance	10

Design principles

Explicit activation
The feature is disabled by default. A policy approval gate must be completed before a device can be authorized.

Visible kiosk session
An operator opens the session once. It scans employees automatically and stops when the attendance window is closed.

Scoped matching
Face-only searches never compare against every company employee—only active enrollments in the assigned branch.

Safe rejection
Low-quality, spoof-like, below-threshold, and ambiguous matches fail without guessing or revealing candidates.

Work completed

1

Tailwind administration page
Policy management, DPO approval, thresholds, device authorization, enrollment, revocation, status summaries, and audit visibility.

2

Login-page kiosk
A clean modal available only to an authorized browser, with privacy notice, fallback, camera guidance, and punch confirmation.

3

Encrypted enrollment
Face embeddings are generated in the browser and encrypted with AES-256-GCM before database storage.

4

Face-only identification
Optional 1:N matching removes employee-ID entry while retaining company, brand, branch, threshold, and ambiguity boundaries.

5

Authorized kiosk devices
Random, expiring, revocable browser credentials stored as hashes and delivered in protected cookies.

6

Attendance integration
Successful matches write into the existing attendance schedule, late, undertime, and credit calculations.

7

Retention automation
A scheduled command erases expired biometric ciphertext and removes old challenges and verification events.

8

Performance tuning
Background preload, face-only warm-up, lighter camera input, model caching, and a slower eye-close action improve kiosk reliability.

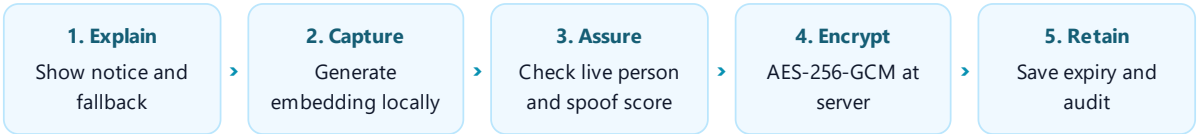
Controls added to the admin policy

Control	Purpose	Default
Main enablement	Turns facial attendance on for the selected brand.	Off
Face-only identification	Allows branch-scoped matching without employee ID.	Off
Similarity threshold	Minimum score required for a face match.	0.55
Ambiguity margin	Minimum lead of best candidate over second best.	0.08
Liveness / anti-spoof	Minimum assurance scores accepted by the server.	0.60 / 0.60
Retention	Defines expiry for templates and verification events.	365 days

Administrators open [Settings → Facial Attendance](#) . Authorized employees use the facial-attendance panel on the login page after the admin logs out.

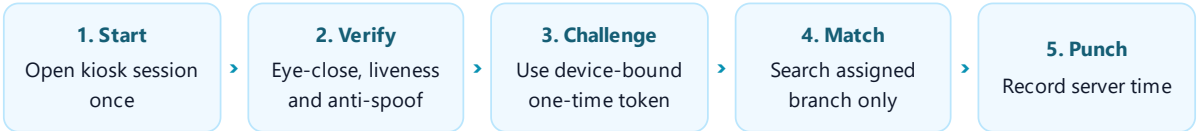
How the system works

Enrollment



An enrollment belongs to the employee's company, brand, and assigned branch. Re-enrollment revokes the former template and erases its ciphertext.

Face-only attendance



Decision rules

Check	Accepted when	Failure behavior
Device	Token is valid, active, unexpired, and branch-bound.	Kiosk panel is unavailable or request is denied.
Challenge	Hash, device, expiry, and unused state are valid.	Request is rejected; token cannot be replayed.
Live person	Eye-close signal and configured assurance scores pass.	Employee is told to retry or use fallback.
Similarity	Best score meets the configured threshold.	No employee identity is disclosed.
Ambiguity	Best score leads the second result by the margin.	System refuses to guess.
Duplicate	No accepted punch for employee/device in prior 60 seconds.	Duplicate punch is rejected.

Attendance slot order



The first empty slot is filled. The system then recalculates the existing schedule, rendered time, lateness, undertime, deductions, and credited days.

Privacy and security controls

Data minimization

- Camera frames are processed locally in the browser.
- Raw photographs are not uploaded or stored.
- The submitted numerical embedding is not written to event logs.
- Rejected 1:N scans do not disclose nearby candidates.
- The camera operates only while the visible automatic kiosk session is open.

Access boundaries

- Admin functions require an authorized admin role.
- All administration is scoped to the selected brand.
- A kiosk is assigned to one branch.
- Device credentials expire and can be revoked remotely.
- Cross-origin requests require an exact configured HTTPS origin.

Credential and template protection

Item	Protection
Kiosk token	32 random bytes; only SHA-256 hash stored; raw token delivered in an <code>HttpOnly</code> cookie.
Same-origin cookie	<code>SameSite=Strict</code> ; secure flag applied when HTTPS is detected.
Approved cross-origin cookie	Exact allowlisted HTTPS origin with <code>Secure</code> ; <code>SameSite=None</code> .
Face template	AES-256-GCM ciphertext with separate IV and authentication tag.
Challenge	Random secret represented by a stored SHA-256 hash; expires after two minutes and is one-use.
Event	Stores decision metadata and scores, not raw frames or embeddings.

Do not weaken thresholds to hide errors

A lower threshold may reduce false rejections while increasing false acceptance. Changes must be evaluated using representative staff, actual kiosk cameras, different lighting, and documented acceptance criteria.

Retention

The daily purge cryptographically erases expired templates, removes challenges expired for more than one day, and deletes verification events according to each brand's configured retention. The non-biometric attendance record follows the organization's separate attendance policy.

Administration guide

A. Install and configure

1. Verify the existing attendance schema.
2. Run the idempotent facial-attendance installer.
3. Create a dedicated encryption secret and place it in the ignored local privacy configuration.
4. Use HTTPS for every production camera page.
5. Schedule the retention command to run daily.

```
php backend/scripts/check_facial_attendance_prerequisites.php
php backend/scripts/install_facial_attendance.php
php backend/scripts/purge_facial_attendance_data.php
```

B. Approve and save the policy

1. Select the intended brand.
2. Open **Settings** → **Facial Attendance**.
3. Enter the approved notice version/text, lawful-basis and PIA references, DPO contact, fallback, and retention.
4. Set thresholds based on pilot evidence.
5. Enable facial attendance, confirm DPO/legal approval, and save.
6. Enable 1:N separately only if the approved material explicitly covers face-only identification.

Built-in validation

The notice requires at least 160 characters, fallback at least 40 characters, retention 1–3650 days, valid threshold ranges, non-placeholder policy content, an encryption key, and approval confirmation.

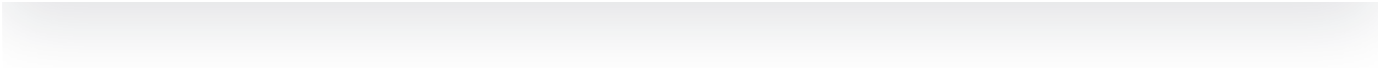
C. Enroll employees

1. Select an active employee with an assigned branch.
2. Explain the approved notice and usable fallback.
3. Record acknowledgment and capture a live face under good lighting.
4. Confirm that the admin page shows an active enrollment and expiry date.

D. Authorize a kiosk

1. Use the physical browser that will operate as the kiosk.
2. Enter a clear device name and select its actual branch.
3. Choose an authorization period and activate the browser.
4. Log out to expose the kiosk panel on the login page.

Revoke lost, repurposed, or untrusted browsers immediately from the active-device list.



Employee kiosk guide

Face-only mode

1. Open **Facial attendance** on the login page.
2. Review the privacy notice if needed.
3. Stand in front of the camera; the active session starts automatically.
4. Keep one face centered and move close enough.
5. Close both eyes for one second when prompted, then open them.
6. Wait for the confirmed employee name and punch slot, then step away. After 2.5 seconds, the kiosk prepares for the next employee automatically.

Employee-ID mode

1. Open **Facial attendance**.
2. Select your enrolled record from the branch-scoped dropdown.
3. Confirm the displayed employee.
4. Start the secure face scan.
5. Complete the eye-close instruction.
6. Wait for server confirmation.

Camera positioning

Light from front

Avoid a bright window behind the employee. Use steady, even lighting.

One person

Keep other faces outside the camera square during the live scan.

Close enough

The face should occupy a useful part of the frame without being cut off.

The fallback is part of the system

If the employee cannot or should not complete biometric scanning, follow the displayed non-biometric attendance instructions. Repeated scanning is not a substitute for a workable fallback.

Understanding messages

Message	Meaning and action
Center your face	No single usable face is visible; adjust position.
Only one person may be visible	Ask others to move outside the camera view.
Move closer	The detected face is too small for dependable processing.
Close both eyes	Hold both eyes closed for about one second, then reopen.
Confidence stayed too low	Improve lighting, remove glare, retry once, or use fallback.
Could not identify confidently	No safe unique match was found; use fallback rather than guessing.

Technical reference

Frontend modules

Module	Responsibility
FacialAttendanceAdmin.jsx	Tailwind administration, policy, enrollment, devices, and audit UI.
FacialKioskPanel.jsx	Login-page panel, privacy notice, challenge, identification, and result flow.
FaceCapture.jsx	Camera lifecycle, model status, capture action, and local error display.
facialEngine.js	Human model preload, detection, face mesh, embedding, liveness, and anti-spoof.
public/face-models/	Locally hosted model manifests and weights.

Backend modules

Module	Responsibility
_common.php	Validation, encryption, similarity, kiosk cookie/origin, scope, and audit helpers.
device_status.php	Determines whether the browser is an active kiosk and returns policy display data.
challenge.php	Rate-limited, device-bound, short-lived one-use challenge creation.
punch.php	Assurance validation, 1:1 or 1:N matching, ambiguity rejection, and event recording.
attendance_apply.php	Existing attendance slot and schedule/penalty integration.
admin/	Admin role gate, settings, device, enrollment, and revocation endpoints.

Database tables

facial_attendance_settings	facial_attendance_devices	employee_face_templates	facial_attendance_challenges
facial_attendance_events	facial_attendance_audit		

Important operational limits

- Challenge validity: two minutes.
- Challenge rate: maximum 10 per device per minute.
- 1:N candidate limit: 500 active templates per branch.
- Duplicate accepted punch window: 60 seconds.
- Device authorization: 1–365 days.
- Policy retention range: 1–3650 days.
- Authoritative timezone: Asia/Manila.

Performance and troubleshooting

Why the first scan can be slower

The first authorized kiosk visit loads and initializes approximately 10 MB of local face models. The implementation now begins this work in the background on the login page. Later scans in the same session reuse the initialized engine.

Problem	Resolution
Employee dropdown appears	1:N is off. The list includes only active facial enrollments in the kiosk branch. Enable 1:N separately to remove selection.
Feature is not installed	Run <code>php backend/scripts/install_facial_attendance.php</code> .
Feature is not enabled	Complete valid policy content, encryption, approval, and main enablement.
Branch selector is empty	Confirm an active branch belongs to the currently selected company and brand.
Cross-origin request denied	Use the Vite API proxy locally; in production allowlist only the exact HTTPS frontend origin.
Challenge could not be created	Check PHP logs, migrations, device state, branch scope, and active enrollment.
Model loading is slow	Keep the login page open briefly; verify static model responses and production caching.
Eye-close check times out	Close both eyes for a full second; improve lighting and camera position.
Missing <code>vite.svg</code>	Clear old site data/service worker once and hard-refresh; dev PWA registration is disabled.

Performance changes made

- Preload engine after active kiosk status is known.
- Use face-only warm-up rather than full-model warm-up.
- Disable the iris model because the face mesh supplies the eye-close gesture.
- Request a 480 x 480 camera stream instead of 720 x 720.
- Use a lightweight face-mesh stage for the eye-close gesture, followed by one full descriptor, liveness, and anti-spoof stage.
- Run the independent full-stage models through the library's supported asynchronous path.
- Do not reuse descriptor or assurance results across employees.
- Allow 45 seconds for capture while returning more specific failure messages.
- Reset failed model initialization so a subsequent scan can retry.
- Display separate local-scan and server-match timings after success.

Escalate persistent slowness with evidence

Record kiosk CPU/GPU, browser version, camera resolution, model request timing, inference messages, lighting, and approximate seconds to first and subsequent scans. This distinguishes network loading from device inference and match-server latency.

Testing and acceptance

Verification already performed

- Idempotent migrations executed against local MariaDB.
- Identification columns and nullable no-ID challenges verified.
- PHP syntax checks passed for facial-attendance endpoints.
- Targeted ESLint checks passed for the React modules.
- A complete Vite production build succeeded.
- Employee/template SQL joins were corrected for database collation differences.

Production acceptance checklist

- ☐ DPO/legal approval and the PIA are documented.
- ☐ The notice accurately describes the selected 1:1 or 1:N behavior.
- ☐ A practical non-biometric fallback is available without retaliation or undue delay.
- ☐ The dedicated encryption key is securely configured and recoverably managed.
- ☐ HTTPS and exact frontend origins are configured.
- ☐ Each kiosk is assigned to the correct branch and expires appropriately.
- ☐ Only intended employees are enrolled and acknowledgment is recorded.
- ☐ False acceptance and rejection are measured with representative participants.
- ☐ All four attendance slots and schedule calculations are verified.
- ☐ Ambiguous, spoof, duplicate, expired, revoked-device, and revoked-template cases are tested.
- ☐ The purge job is scheduled, monitored, and tested.
- ☐ Incident, access-review, employee-request, and revocation procedures are exercised.

Known limitations

- Browser liveness and anti-spoof are MVP controls, not certified presentation-attack detection.
- 1:N comparison is synchronous and linear, with a 500-template branch cap.
- First-time performance depends on kiosk hardware and model delivery speed.
- Thresholds require organization-specific validation.
- Hands-free scanning is active only while the visible kiosk window remains open; closing it stops the camera and retries.
- The attendance policy currently fills four daily slots sequentially.

Recommended rollout

Begin with a supervised pilot, preserve the fallback, monitor failures without pressuring employees, review demographic and environmental performance, and obtain final DPO/legal sign-off before broader production use.

Source guide: `docs/FACIAL_ATTENDANCE_IMPLEMENTATION.md`

Deployment gate: `docs/FACIAL_ATTENDANCE_DEPLOYMENT.md`

