INFORMATION
COMMUNICATION
ENTERTAINMENT

A PROPOSAL FOR THE RAILWAY ADMINISTRATION

Technical compliance and value-added capabilities

ICE Passenger Platform · 16 November 2026

10 / 10 tender clauses met (sections B and C)	**28** capabilities beyond the tender, at no extra cost	**99.5%** monthly uptime, reported automatically	**₹0** capex for Railways

PURPOSE

Every tender requirement met, and more than 25 capabilities added

ICE (Information · Communication · Entertainment) meets every requirement in sections B and C of the licence document. It also adds more than 25 capabilities beyond the tender at no extra cost to Railways.

ICE is a passenger platform that opens from a QR code on any mobile browser. Passengers ask questions and get answers, receive Railways alerts, and watch or listen to entertainment, with no app to download. The licensee designs, deploys, operates and maintains the platform and funds it through advertising.

This document sets out how each tender clause is met, what Railways receives beyond the tender, how the platform is built and hosted, and how Railways keeps oversight.

SECTIONS B AND C

Compliance with the tender

ICE complies with all ten clauses. The table shows how each one is met.

Clause	Requirement	How ICE complies
B.1	**No-app access via PWA or mobile browser, Android 10+ and iOS 15+**	✓ Complies Built as a progressive web app that opens straight from the QR code. Passengers can optionally add it to the home screen. Every release is tested on real Android 10 and iOS 15 devices before going live.
B.2	**99.5% availability per month; licence-fee credit for downtime beyond the SLA**	✓ Complies Two or more application servers behind a load balancer, a managed database with a standby copy, and releases with no downtime. Independent external monitoring checks the platform every minute, and the monthly uptime report goes to Railways automatically.

Clause	Requirement	How ICE complies
B.3	End-to-end HTTPS, OWASP Top-10, DPDP Act 2023, IT Act 2000	✓ Complies HTTPS everywhere with modern TLS and strict security headers. Protection against every OWASP Top-10 category is built into the framework and covered by tests. A security audit by a CERT-In empanelled auditor is completed before go-live and repeated every year. DPDP measures are listed under Value-added capabilities.
B.4	Government of India IT policy and MeitY cloud guidelines	✓ Complies Hosted only on a MeitY-empanelled cloud service provider in an Indian region. All passenger data, logs and backups stay in India.
C.1	30-second 2D/3D English video on passenger welfare schemes in year one	✓ Complies Produced by the licensee in year one and submitted to Railways for approval. It is shown in the reserved public-service airtime at no cost to Railways.
C.2	Prior written approval for every advertising campaign	✓ Complies No campaign can go live without approval. Each campaign moves through a built-in workflow (draft, submitted, approved or rejected) in which the Railways officer approves it. Each approval is recorded with the officer's name, date and time.
C.3	Railways priority override for public-service and emergency messages	✓ Complies Authorised Railways officials can send a message to a chosen train, station, division or zone. It appears on passengers' screens within seconds and takes priority over all advertising.
C.4	Up to 10% of display time reserved for public-interest messages at zero cost	✓ Complies The ad scheduler reserves Railways' share before selling any airtime. It records actual display time, and the monthly report shows the share delivered.
C.5	Ban on obscene, offensive, political, religious, defamatory, competitor-to-Railways or unlawful content	✓ Complies All ads and content are checked before publishing. The AI assistant is restricted to travel and service topics, and declines political, religious and other prohibited subjects. Railways can remove any item instantly.
C.6	Licensee responsible for content licensing, copyright and piracy disputes	✓ Complies Every title carries a recorded licence and expiry date and is taken down automatically when its licence ends. Video links expire and cannot be shared, and studio content is protected with industry-standard DRM. Takedown requests are handled within a defined response time.

BEYOND THE TENDER

Value-added capabilities, at no extra cost

ICE adds 28 capabilities that the tender does not ask for. They give Railways more control, stronger security and better evidence of performance. All are included in the licence at no cost to Railways.

Control and oversight 6

01 Hierarchical role-based access control (RBAC) with jurisdiction scoping across Zone, Division and Station
Each official sees and acts only on their own jurisdiction

02 Segregation-of-duties (SoD) model with tenant-level data isolation for advertisers
Clear separation of duties; advertisers never see passenger data

03 Real-time application performance monitoring (APM) and observability dashboard
Live view of usage, response times and errors at any moment

04 Append-only, tamper-evident (hash-chained) audit trail with forensic export
Who did what and when, provable and exportable for vigilance or audit

05 Feature-flag-driven progressive delivery with jurisdiction-scoped canary rollouts and an instant kill switch
Features go live on one route first and can be withdrawn in seconds

06 Rules-based campaign orchestration engine with time, train and station triggers
Welfare and safety campaigns run automatically, such as festival-rush advisories

Security 7

07 Multi-factor authentication (MFA, TOTP) for all privileged accounts
Accounts stay protected even if a password is stolen

08 Brute-force and abuse protection: progressive account lockout and per-endpoint API rate limiting
Protection against password guessing and automated abuse

09 Step-up authentication for privileged operations
No one can approve or broadcast from an unattended screen

10 Cryptographically signed, time-bound approval URLs (HMAC-SHA256)
Email approvals cannot be forged, altered or reused

11 Field-level encryption at rest (AES-256) and encrypted backups
Data stays unreadable even if storage is compromised

12 Centralised security event logging with 180-day in-India retention and SIEM-ready export, aligned with CERT-In directions
Ready for incident investigation; logs can feed Railways' security monitoring

13 Tokenised, time-limited media URLs with anti-hotlinking controls
Licensed content cannot be hotlinked or redistributed

Data protection 6

14 **Privacy-by-design architecture: anonymous-first sessions and data minimisation**
No login needed to ask, read alerts or watch; minimal personal data collected

15 **Data Principal self-service portal for access, correction and erasure requests**
Passenger rights under the DPDP Act met without paperwork

16 **Automated data-lifecycle management with policy-driven retention and purge**
Nothing is kept longer than needed

17 **Granular, multilingual consent capture with consent audit logging**
Informed consent, recorded as the DPDP Act requires

18 **Privacy-preserving contextual advertising: no behavioural profiling, child-safe ad delivery under Section 9 of the DPDP Act**
Ad model stays within the DPDP Act's protections for children

19 **Multi-channel incident and breach notification workflow (email, SMS, in-app)**
Prompt notice to Railways, users and authorities if an incident occurs

Reliability 4

20 **Synthetic monitoring with health-check probes at one-minute intervals**
Problems are caught and fixed before passengers notice

21 **Asynchronous job queues with automatic retry, back-off and dead-letter handling**
Alerts and reports are never silently lost

22 **High-availability database with standby replica, point-in-time recovery (PITR) and routinely restore-tested backups**
Fast recovery from hardware or data failure

23 **Graceful-degradation maintenance mode with passenger-facing status notices**
No confusing errors during upgrades

Integration 2

24 **Versioned RESTful APIs documented to the OpenAPI 3 standard, with token-based authentication, for Railways systems (such as NTES, Rail Madad and PRS), subject to Railways approval**
Ready to connect official train-running and grievance data when Railways permits

25 **CI/CD pipeline with automated unit, integration and end-to-end browser test suites**
Fewer defects reach passengers

Passenger experience 3

26 **Internationalisation (i18n) framework: English and Hindi at launch, plus the regional language of each operating zone**
Passengers read alerts and answers in a language they know

27 **Offline-first progressive web app with service-worker caching, optimised for low-bandwidth networks**
Usable at stations and on routes with poor signal

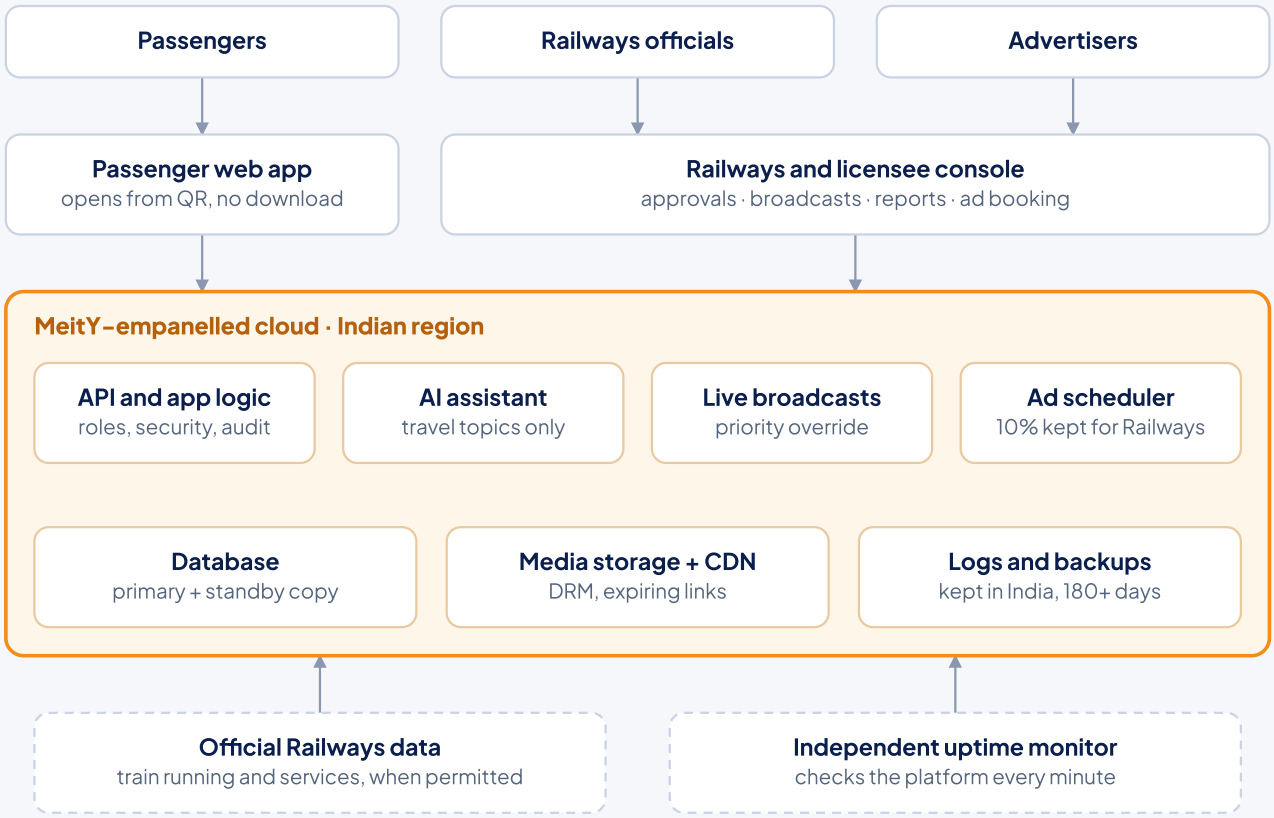
28 **Accessibility compliant with GIGW 3.0 and WCAG 2.1 AA**
Usable by passengers with visual or motor impairments

HOW IT IS BUILT

Platform architecture

ICE runs entirely on a MeitY-empanelled cloud in an Indian region, so all passenger data, logs and backups stay in India.

Every ICE component runs on a MeitY-empanelled cloud in India



Passengers use a light web app that opens from the QR code. Railways officials, licensee operators and advertisers each work in one console, with access set by their role. The AI assistant answers only from approved Railways information and declines topics outside travel and services.

The platform is built on mature, widely used open-source web technology with long-term support and a large pool of skilled engineers in India. Railways is not tied to any proprietary licence.

OVERSIGHT

Governance and reporting to Railways

Railways receives a standard set of reports automatically, and can see live figures at any time in its own console.

Report	Frequency	Contents
SLA and uptime report	Monthly	Availability against the 99.5% target, each outage with its cause and duration, and any licence-fee credit due

Report	Frequency	Contents
Public-service airtime report	Monthly	Display time delivered to Railways messages against the 10% reservation, by zone and division
Campaign approvals register	Monthly, and on request	Every campaign submitted, the approving officer, date of approval or rejection, and run dates
Emergency and priority broadcasts log	Monthly, and on request	Each broadcast with sender, audience, time sent and reach
Usage report	Monthly	Scans, questions answered, alerts delivered and content viewed, by station and train
Content licence register	Quarterly	Licensed titles, rights holders, licence periods and takedowns
Security report	Annually, and after any incident	CERT-In empanelled audit findings and their closure, plus any incidents and actions taken

Railways can remove any advertisement or content item, pause a campaign, or send a priority message at any time without going through the licensee.

NEXT STEPS

Proposed pilot and next steps

We propose a 90-day pilot on a small set of trains and stations chosen by Railways, at no cost to Railways.

1. Railways selects the pilot trains and stations and nominates an approving officer.
2. The licensee places QR codes on seats, coaches and platforms in the pilot, with Railways' permission.
3. The platform goes live with information, alerts and entertainment. All campaigns are approved through the console from day one.
4. Railways reviews the monthly reports listed under Governance and reporting and the pilot's results: usage, uptime, approvals and passenger feedback.
5. After the review, the licensee and Railways agree the rollout across further zones.

To start the pilot we need three things from Railways:

- **Permission to place QR codes in the pilot trains and stations**
- **A nominated approving officer for campaigns and content**
- **Access to official train-running and service information (for example through NTES), so that answers come only from authoritative data**