Security Overview

Public operational security summary for the Instant Settlement Payment Gateway website and enquiry channel.

1. Scope

This document covers the public marketing site and commercial enquiry route. Detailed payment processing security, certifications, partner responsibilities and incident terms are supplied during due diligence and in the applicable merchant agreement.

2. Website controls

- HTTPS with strict transport security on the canonical domain.
- Content Security Policy, frame blocking, MIME sniffing protection and restricted browser permissions.
- Same-origin contact submissions with input length controls, validation and a hidden bot field.
- Rate limiting based on a one-way IP hash.
- D1 storage binding for submitted commercial enquiries.

3. Data handling

The contact form is not a payment form. Do not submit card numbers, bank credentials, passwords, authentication codes or other payment secrets. Enquiry records are limited to business contact and service-scoping data.

4. Payment service due diligence

Before live processing, the parties may review KYB/KYC requirements, payment methods, data flows, integration boundaries, authentication, refunds, disputes, access controls, reporting and incident contacts. Availability and responsibilities are documented for the approved service configuration.

5. Responsible reporting

If you believe the public site has a security issue, email contact@instantsettlementpaymentgateway.com with the affected URL, a clear description, reproduction steps and impact. Do not access data that is not yours or disrupt the service while testing.

Effective date: 22 July 2026. This document is provided for operational transparency and has not been presented as lawyer-reviewed advice.