External API Gateway and Integration Standards

Document ID: IE-APS-2025.01
Version: 1.0
Effective Date: 2025-11-01
Department: IT & Engineering - R&D

1. Objective

To define the requirements for all externally exposed APIs to ensure security, high performance, version control, and clear documentation for clients.

2. API Design and Documentation

- **RESTful Standard:** All APIs must follow a consistent, RESTful design approach, using standard HTTP methods and status codes.
- **Versioning:** All major API changes require a new version number (e.g., /v2/). Older versions must be supported for a minimum of **12 months** after the release of a new major version, with clear deprecation warnings.
- **Documentation:** All APIs must be documented using an industry-standard specification (e.g., OpenAPI/Swagger) and publicly hosted on the developer portal.

3. Security and Authentication

- **Authentication:** All external API endpoints require strong, token-based authentication (e.g., OAuth 2.0 or secure API keys). Basic authentication is prohibited.
- **Rate Limiting:** Mandatory rate limiting must be configured at the API Gateway to protect against DoS attacks and ensure fair usage across all clients. Standard limit: **[1000 requests per minute]** per client key.
- **Input Validation:** Strict server-side validation and sanitization of all input parameters is required to prevent injection attacks (e.g., SQLi, XSS).

4. Performance and Data Handling

- **Latency:** The target median API latency (P50) is **< 100 milliseconds**.
- **Payloads:** Payloads must be efficient (JSON format, gzip compression encouraged). Sensitive data returned in API responses must be minimal and encrypted in transit (per **Data Encryption Standard**).