SAP API Policy

This API Policy standardizes the use of application programming interfaces, extensions, and related data transmission interfaces made available as part of SAP solutions ("APIs") and forms part of the Documentation for the SAP solution with which it is provided. It explains API availability and API limits, and establishes controls designed to safeguard solution health and security, promote equitable access, prevent API misuse, and support the enforcement of this API Policy.

1. API AVAILABILITY

1.1. **Published APIs.** APIs published on the SAP Business Accelerator Hub (also called "API Hub") or otherwise identified in product-specific Documentation ("Published APIs") are made available for the purposes described in that Documentation such as to integrate SAP applications with customer or third-party solutions, build extensions, synchronize data, exchange data, trigger events, or similar business scenarios ("Documented Use").

1.2. **Non-Published APIs.** Customer and third-party applications must not access, invoke, or interact in any manner with APIs that are not Published APIs, in particular those that are labeled internal, private, or with a similar designation or APIs bound to SAP-reserved clients (e.g. SAP reserved-client namespaces in S/4HANA) except as permitted by the Documentation or otherwise authorized by SAP (e.g., customers may use custom-developed ABAP interfaces in private cloud and on-premise deployments). These interfaces may change or be removed without notice. Customers and partners are required to verify that each endpoint for Documented Use is a Published API.

2. API CONTROLS

The following Specific and General Controls apply to API use (collectively, "API Controls"):

2.1. **Specific API Controls.** SAP documents and maintains specific API controls in the applicable product-specific Documentation or API Hub for each API, including:

- functional / technical use rate limits and quotas,
- deprecation schedules,
- data ingress/egress quotas,
- limits and preconditions for bulk extraction / replication, and
- other security/technical requirements.

2.2. **General API Controls**

2.2.1. SAP prohibits any API use for purposes of: (a) competitive analysis, (b) enabling functions or scenarios that are not part of the Documented Use unless otherwise authorized by SAP, or (c) in a manner that creates a risk to system performance, stability, or security.

2.2.2. Except through and within the limits of SAP-endorsed architectures, data services, or service-specific pathways expressly identified and intended for such purposes, SAP prohibits API use for: (a) interaction or integration with (semi-) autonomous or generative AI systems that plan, select, or execute sequences of API calls, and (b) scraping, harvesting, or systematic and/or large-scale data extraction or replication.

3. MONITORING AND REMEDIES

SAP may monitor API usage and take reasonable enforcement actions, including throttling, suspension, or termination of access in the event of non-compliance with the Documentation (including this API Policy). Customers, partners, and third parties must not bypass, disable, or otherwise circumvent API Controls,

including through intermediary services, custom code or developments, proxies, gateways, impersonation techniques, or similar mechanisms.

4. COMPLIANCE

This API Policy does not limit SAP's obligations to provide any data export or other data egress capabilities that may be expressly required by law, including obligations related to data portability, switching, or legal record retention.