Purpose

At Elanco, deployment of any solution in a stable, scalable, and secure way is the responsibility of everyone involved in the development of applications. Elanco has documented our Supplier Obligations (see Appendix A) and created a set of Architecture Declarations (below) to ensure robust cloud-native applications with quality code and sustainable run rates. Suppliers with this skillset may also choose to participate in a Preferred Application Development Program (see Appendix B). Elanco developers will work with you to explore design options to help facilitate these within the solution.

Scope

The scope of this document only applies to applications which require any custom infrastructure to be built to support the end-to-end solution and does not apply to SaaS offerings, such as Workday or DocuSign.

Architecture Declarations

The following declarations build on the Elanco IT Enterprise Architecture Principles, helping to direct solution decisions, unlocking value through standardization that drives cost savings, whilst promoting consistent compliance and security, as well as reducing the impact of technical debt.

#	Type	Declaration
1	Hybrid Multi-Cloud	By default, **commodity and/or highly-industrialized business processes must target Software-as-a-Service (SaaS). Public Cloud must be prioritized for all other IT solutions,** following the Enterprise Architecture Public Cloud Positioning. **Colocation Data Centers and the Edge (Local Site) hosting must be reserved for specialist solutions** (Research & Development and Manufacturing) with specific business requirements.
2	Open Source	By default, **solutions must prioritize cloud-agnostic, open-source technologies**, with any use of proprietary technologies looking to maximize our strategic investments (e.g., Microsoft, Google, SAP, etc.).
3	Custom Developed	By default, **custom developed solutions must embrace a Cloud Native architecture** (Twelve-Factor App), specifically **ephemeral (short-lived) and stateless (does not persist a session), running in a container (Open Container Initiative)**.
4	Applications	By default, **solutions (Custom Developed, COTS, and Data Assets) must be provisioned, maintained and supported via a pre-approved automation pattern.** If a pattern does not exist, **Infrastructure-as-Code (Hashi Corp Terraform and Red Hat Ansible) must be leveraged to provision, maintain and support, ensuring recoverability, as well as consistent enforcement of compliance and security controls.**
5	DevSecOps/FinOps	**All systems must be continuously maintained, with a focus on cost optimization, compliance and security advisories.** System owners must demonstrate a timely response to all Critical/High advisories.
6	Data Foundation	Where appropriate, **solutions and data assets must consume and/or contribute to the Elanco Enterprise Data Foundation**, especially the domain-based architecture, where each domain represents a related set of enterprise data.
7	Web-First	By default, **solutions must be consumable via the web (browser-based)**, avoiding the use of traditional client-side software and/or proprietary plugins (e.g., Dot Net Framework, Java, Flash, etc.). If client-side software is required, it must be managed/protected by the enterprise Endpoint Management solution (e.g., Microsoft Endpoint Manager).
8	API-First	By default, **solution interoperability must occur via open and documented web service-based APIs** (e.g., REST, GraphQL, gRPC, etc.). Any legacy system-to-system integrations must leverage the approved Enterprise Integration Middleware (e.g., Boomi, Azure Logic Apps, etc.).
9	Internet-First	By default, **solutions must be accessible via the Internet, with Transport Layer Security enabled.** Any non-Internet accessible solution must be restricted to Cloud-PC (e.g., Windows 365) or a fully managed endpoint via the Enterprise Client Virtual Private Network (e.g., Palo Alto Prisma Access).
10	Identity	By default, **solutions must integrate modern authentication and authorization (Elanco ID and MFA)**, with conditional access controls that enforce the principles of least privileged access. Basic/legacy authentication and authorization techniques must be avoided, including IP whitelisting.
11	Information Security	By default, **solutions must adhere to the Elanco Information Security Policy Directives and Standard**, archived via programmatically-defined controls embedded as part of the provisioning pipeline.

Exception Criteria: A priority business-critical requirement, with an approved risk assessment and positive ECE (ROI), that can only be achieved via the exception.

Enterprise Principles

We aren't intending to 'reinvent the wheel' with our Engineering Standards, therefore where possible we borrow from leaders in the field.

We expect the quality of code written by vendors and Elanco internal employees to be comparable.

Engineering practices largely follow Google's Engineering Practices Documentation.

Elanco Developer Guides can be found on Elanco's Developer Portal (available to onboarded Suppliers).

The core skills Elanco expects in application development include:

- Agile Practices
- Continuous integration and continuous development practices
- Leverage our Infrastructure as Code (IAC) offerings (Horizon)
- Modernizing legacy code, and ensuring new code developed is of modern standards
- Cloud-Native application development
- User experience (UX) best practices to be adhered to, and key UX flows to be documented
- Decoupled Apps, APIs, and Services
- Application security and access. Applications should be maintained with no critical security alerts, appropriate authentication should be applied.
- Error handling, alerting and monitoring

Web Standards

Capability	Priority	Minimum Supported
Customer Identity	Very High	SAP CDC
Secret Storage	High	Google Secret Manager or Azure Key Vault
Security Standards	High	OWASP Top 10
Containerization	High	Docker/Horizon pattern
Code Quality	High	ESLint, Google's Engineering Practices Documentation
E-mail Services	Medium	SendGrid
Front-end Framework	Medium	Next.js
Server-Side Runtime	Medium	Node.js
Testing	Medium	Lighthouse, Jest, Testing Library, Playwright, Cypress.io, Storybook
Documentation	Medium	Elanco Developer Portal (available to onboarded Suppliers), application's README
API Format	Low	REST
API Documentation	Low	Swagger

Appendix A: Supplier Obligations
All Supplier's obligations under the Agreement are in addition to the requirements of this document.

1. Suppliers must attest that they are fully able to meet the requirements, standards, and expectation outlined in this document.

2. Where possible, Suppliers must use Elanco's existing design patterns which can be shared with you by an Elanco employee. For development teams this means:
    a. Supplier must have experience deploying Cloud Infrastructure leveraging appropriate Infrastructure as Code (IaC) frameworks (specifically Terraform) to deploy programmatically.
    b. Supplier must have experience deploying Cloud Infrastructure as part of the CI/CD process (e.g., Azure Pipelines/Github Actions).
    c. Low-code/No-code tools (e.g., Microsoft PowerApps, Google AppSheet) should not be a proposed solution.
    d. Where possible, Supplier should have experience with deploying applications within a regulated environment (controlled, tested, and qualified deployments).
    e. If applicable, Supplier must follow the Elanco Web Standards (Appendix A) for languages/tools and documentation best practices.

3. Application development should occur locally or using cloud-based tools, such as Github Codespaces.

4. All application, infrastructure, and configuration code must be stored, maintained, and deployed from Github.

5. All proposed solution designs must be submitted to Elanco for Architecture Review to ensure that eth solution meets both the original requirements and Elanco's Enterprise Principles.

6. All solutions, unless deemed an exception by our solutions review team, must be deployed in a cloud native architecture (e.g., PaaS-First, FaaS/PaaS).

7. Suppliers must demonstrate an understanding of appropriate security controls when handling Elanco keys/certificate/credentials (Secret Manager/Key Vault integration).

8. Suppliers must follow Elanco's computer system validation requirements for third parties/suppliers (each, a "Third Party/Supplier") with respect to the validation and support of computerized systems as stated in the Information Systems Quality addendum and outlined in our IT Playbook which is available to onboarded Suppliers.

9. Suppliers must propose solutions that are in agreement with Elanco's Information Security Standard as stated in the Supplier Resources on https://elanco.com/en-us/suppliers.

10. Suppliers must propose solutions that are in agreement with Elanco's Supplier Privacy Standard as stated in the Supplier Resources on https://elanco.com/en-us/suppliers.

Appendix B: Preferred Application Development Supplier Status

Elanco now offers a Preferred Application Development Supplier status to Suppliers who can attest that they are fully able to meet the requirements, standards, and expectations outlined in this document. Prior to signing a Statement of Work or other contract with Elanco, the Supplier agrees to submit at least one example of software requirements, software architecture diagrams, and test plans/reports from a previous build for review by our Solution Architects.

Upon approval of this submission, Elanco can then assist with expedited onboarding, keep the Elanco IDs for the supplier's core team in our system, contribute to the supplier's Supplier ratings within Elanco's systems, and ensure that the supplier's preferred status is visible to all Elanco IT. Failure to adhere to the development and process standards in this document could result in delays, penalty fees, and removal from preferred status.