附件 XY

IT 网络安全补充协议

版本 1.2

日期：2026 年 11 月 23 日

定义

就本 IT 网络安全补充协议而言，下列术语具有以下含义：

“适用网络安全法律”是指适用于一方、本服务、相关产品、数据处理活动，或本服务被提供、接收、托管、运营、访问、分发或投放市场所在地区的所有具有约束力的网络安全、信息安全、产品安全、关键基础设施安全、网络事件报告及相关法律、法规、监管要求和强制性标准。

此类法律可包括（仅限于在相关具体情形下适用的范围内）：NIS2 指令（EU）2022/2555 及其各国转化立法、德国《联邦信息安全办公室法》（BSIG）、法规（EU）2022/2554（“DORA”）、法规（EU）2024/2847（“CRA”），以及相关亚太司法管辖区适用的网络安全立法，且均以其不时修订或替代后的版本为准。

本补充协议中对某项法律的引用，其本身不应被解释为表明该法律适用于供应商、本服务或某项特定交易。

“网络安全事件”是指对以下方面产生实际或潜在重大不利影响的任何单一事件或系列事件：(i) 本服务、巴斯夫数据或巴斯夫 IT 系统的保密性、完整性或可用性；或 (ii) 用于提供本服务的网络和信息系统的安全性，包括但不限于未经授权的访问、数据泄露、恶意软件感染、拒绝服务攻击或技术与组织措施（ToMs）遭受的任何其他破坏。

“严重漏洞”是指通用漏洞评分系统（CVSS）评分为 9.0 或以上的任何漏洞，或任何已在现实环境中被积极利用的漏洞（“零日漏洞”）。

“高危漏洞”是指 CVSS 评分为 7.0 或以上但低于 9.0 的任何漏洞。

“分包商”是指供应商或其关联公司为履行本服务的任何部分，或为与本服务相关的处理、存储或访问巴斯夫数据而委托的任何第三方。

I. 网络安全一般规定

1) 网络安全一般要求

各方应遵守在特定司法管辖区内对该方、本服务或相关产品具有约束力的适用网络安全法律。因此，在向巴斯夫提供服务时，供应商至少应实施并维持适当的技术和组织措施、内部控制及信息安全流程（以下简称“ToMs”），以保护其环境中的巴斯夫数据、IT 系统和基础设施免遭意外、未经授权或非法的访问、披露、篡改、丢失或破坏。ToMs 的设计、实施和维护应符合当前技术水平，并应考虑网络和信息系统在保密性、完整性和可用性方面所面临的风险。此类 ToMs 应包括（但不限于）：

治理、风险与合规

a. 对所有可访问巴斯夫数据或巴斯夫 IT 系统的供应商人员定期（每个自然年至少一次）开展网络安全意识培训，包括针对网络钓鱼、社会工程学及凭据安全管理的专项培训；
b. 任命指定的信息安全官或同等职能，负责 ToMs 的实施与监督；
c. 建立并维护符合 ISO/IEC 27001 或同等标准的全面信息安全管理体系（ISMS）；
d. 建立定期评估 ToMs 有效性的程序，例如通过内部审计或外部审查（如 ISO 27001、EN 50600、TISAX 和 SOC 2 Type 2）。

访问与身份管理

a. 实施与风险相适应的访问控制，包括：对所有远程访问以及对关键系统和特权账户的访问实施多因素认证；在雇佣关系终止或变更后二十四（24）小时内撤销访问权限；并基于最小权限原则对特权访问权限进行限制和控制；
b. 实施远程访问策略和技术限制措施，防止远程用户将文件保存至个人设备；

c. 确保在合同关系或雇佣关系终止时及时归还所有组织资产；

d. 巴斯夫数据及其备份在归还后必须彻底删除，并应提供销毁验证报告；

e. 实施身份与访问管理程序，包括定期（至少每季度一次）开展访问权限审查和重新认证。

数据保护与加密

a. 使用加密技术保护巴斯夫数据的保密性、完整性和/或真实性，包括实施书面加密策略，确保所有敏感或机密数据（无论是静态存储、传输中，还是位于供应商设备、存储位置和传输系统中）均采用业界认可的加密算法和协议进行加密（例如，静态数据采用 AES-256，传输中数据采用 TLS 1.2 或更高版本），并配套适当的密钥管理流程，包括密钥轮换、密钥安全存储及书面化的密钥生命周期管理；

b. 识别并分类不得公开的信息，并在组织内部使用数据防泄漏工具；对测试数据进行选择、控制和保护（例如依据 ISO 27002），并禁止使用客户数据；

c. 对存储介质采取安全措施，包括针对可移动介质的专门规定，以及在介质重复使用或处置时保护机密信息的要求。

物理与组织安全

a. 在存储或可获取巴斯夫数据及与本服务相关数据的所有场所采取物理安全措施（例如但不限于：服务器机房和办公室上锁、访客陪同制度）；

网络与系统安全

a. 建立书面流程，确保网络和信息系统在采购、开发和维护（包括补丁管理）过程中的网络安全，包括漏洞管理计划，涵盖：(i) 定期（至少每月一次，面向互联网的系统应持续进行）对供应商系统和解决方案进行漏洞扫描；(ii) 基于风险确定修复优先级；以及 (iii) 在以下时限内完成补丁修复

或缓解：严重漏洞七十二（72）小时内；高危漏洞三十（30）个自然日内；其他漏洞按照风险处置计划处理；

b. 实施网络控制以确保系统和应用安全，包括在网络协议中明确安全机制和服务水平、对用户、服务和系统进行隔离、经风险评估后将网络划分为独立域、管理外部网站访问，以及部署用于内容过滤的互联网代理；

c. 在组织内部对异常行为进行持续且基于风险的监控，包括定期和实时监控、向相关方通报异常事件、在互联网连接处部署 IDS/IPS，以及对收发电子邮件进行自动扫描；在组织网络中部署恶意软件检测系统，包括服务器和工作站的防病毒软件，以及防火墙规则策略；

d. 在组织内部启用事件日志记录，包括启用系统管理日志和网络流量日志、防止用户篡改日志信息、采取保护措施（如加密哈希），并通过安全信息系统（如 SIEM 工具）进行日志分析；

e. 限制可覆盖系统和应用程序的实用工具程序的使用；

f. 实施网络流量过滤和防护措施，包括但不限于：为面向互联网的应用部署 Web 应用防火墙（WAF）、具备反钓鱼功能的电子邮件安全网关，以及基于 DNS 的安全控制。

终端与资产安全

a. 建立终端安全措施，包括：针对纸质文件和可移动存储介质的清洁桌面规则、针对信息处理设施的清屏规则、对场外资产（如 BYOD）的保护，以及制定终端设备安全配置和使用的规则与控制措施，包括防止安装未经授权的软件、BYOD 安全，以及针对无线连接的专门控制；在设备处置或重复使用前，检查并安全清除或销毁机密信息的措施。

云安全

a. 维护符合行业标准（如 ISO 27017、CSA 云控制矩阵）的书面云安全策略；与其他客户的实例进行逻辑隔离（如私有子网，或在合同约定时采用专用租户）；应要求提供证明隔离情况的架构图；并对云加密密钥拥有唯一控制权，或在技术上无法避免时，使用客户管理的密钥并配套书面密钥管理程序。供应商可通过取得并维持有效的 ISO/IEC 27001 认证及其云安全扩展 ISO/IEC 27017 认证，或同等行业标准框架认证，来证明其符合上述要求，前提是该认证范围涵盖本服务。

b. 除上述最低要求外，如事先获得告知，供应商在访问巴斯夫环境或在巴斯夫环境中开展作业时，应遵守巴斯夫适用的安全政策。就供应商自身的相关政策而言，如有任何可能实质性降低本服务安全性的政策变更，供应商应至少提前三十（30）个自然日书面通知巴斯夫。在此情况下，双方应本着诚信原则进行协商，必要时公平调整双方承诺的条款，以妥善应对由此产生的风险。

c. 如巴斯夫数据包含个人数据，上述措施以及合同文件中规定的任何附加安全措施的实施与遵守，旨在为巴斯夫个人数据的处理提供适当水平的安全保障，并应始终符合适用的数据保护法律法规。

2) 网络安全标准的实施

供应商应在适用情况下实施并维持有效的、符合当前技术水平的 IT 安全标准，例如：

a) 最新版 ISO/IEC 27001 及适用的 CMMI（能力成熟度模型集成）标准——适用于基础设施的实施与服务；和/或

b) EN 50600 可用性等级 3（相当于 Uptime Institute Tier 3）——适用于核心数据中心的实施与服务；和/或

c) 依据德国汽车工业协会（VDA）“TISAX”（可信信息安全评估交换）模型取得的认证；

d) 符合《中华人民共和国网络安全法》要求的网络安全等级保护（MLPS）2.0 合规。

3) 主动风险识别与安全威胁管理

作为一项一般性义务，供应商应识别并评估可能影响信息保密性、完整性或可用性的所有风险、威胁和漏洞。供应商还应收集和分析安全威胁信息，以形成相关威胁情报，并开展风险分析，在考虑资产关键性、漏洞及以往事件的基础上，对可能引发损失的潜在事件进行定量或定性评估。

应基于妥善制定并持续维护的书面风险处置计划，选择并实施适当措施，以降低、规避、接受或以其他方式管理信息安全风险。

所有已识别的风险及相关因素（包括但不限于资产价值、潜在影响、威胁、漏洞及发生可能性）均应接受定期监控和审查。

4) 供应商安全风险评估

(1) 巴斯夫与供应商每三年共同对本服务和 ToMs（包括相关接口及与巴斯夫集团 IT 环境的集成）开展一次供应商安全风险评估，该评估由巴斯夫或与供应商不存在竞争关系且负有保密义务的第三方服务提供商执行。

(2) 在供应商安全风险评估期间，供应商有义务提供所有必要的信息和文件，安排相关人员配合，并本着诚信原则予以协作，以便对其服务和 ToMs 进行全面评估。其服务和 ToMs 中已识别的缺陷或薄弱环节应在以下时限内完成整改：(i) 对巴斯夫、其基础设施或其数据安全构成紧迫风险的严重漏洞或缺陷：七十二（72）

小时内完成整改；如在该期限内技术上无法完成整改，则应在该期限内实施有效的临时缓解措施，并在合理可行的情况下尽快完成全面整改；(ii) 高危漏洞或重大缺陷：三十（30）个自然日内；(iii) 其他缺陷：按照双方商定的整改计划执行。如出现反复发生或未能解决的重大缺陷，是否继续与供应商合作由巴斯夫在综合考虑缺陷的严重程度和性质后合理决定。

(3) 如在供应商安全风险评估期间发现，无法在合理期限内充分缓解或被巴斯夫接受的重大风险或漏洞，应针对此类风险制定改进计划。供应商同意积极配合并努力落实该改进计划。

(4) 如供应商未能在规定时限内落实约定的整改措施，或经合理努力后风险仍处于不可接受的高水平，巴斯夫保留在事先书面通知并考虑风险严重程度后采取以下措施的权利：

- 暂停受影响的服务，
- 限制特定服务或接口，
- 停止支付或按比例减少支付与受影响服务相对应的款项，或
- 因故终止本协议或任何单项协议。

(5) 在行使终止权之前，双方应穷尽所有合理的替代方案以缓解风险，并启动向高级管理层的升级处理。

5) 网络安全审计

(1) 在本协议有效期内，经巴斯夫提前十五（15）个工作日以文本形式发出书面通知后，供应商应在正常工作时间内（如为监管机构，则在该监管机构要求的任何时间），向巴斯夫、巴斯夫代理人及任何监管机构（统称“审计方”）提供，并促使所有供应商关联公司和/或供应商代理人提供以下访问权限（包括其可能合理需要的任何协助）：供应商场所和/或供应商关联公司场所及其他场所、供应商系统及其他 IT 和通信系统、人员、文件、第三方认证（包括相应审计报告）、数据及数据载体，前提是上述各项 (i) 处于其控制范围内；(ii) 与本服务相关；且 (iii) 适合用于开展审计、评估、审查和/或检查，以核实本附件（网络安全）中有关网络安全的信息与 IT 安全要求的遵守情况（“审计”），尤其是：

a) 审查供应商和/或供应商关联公司对本服务的履行情况及对本协议条款的遵守情况，包括在适用于本服务的范围内的运营、安全、质量及其他方面，特别是：(i) 供应商的实践和程序；(ii) 供应商系统；(iii) 有关服务水平及其他绩效标准合规情况的支持性信息和计算；(iv) 落实相关安全控制、实践和程序的一般控制；以及 (v) 灾难恢复和备份程序；以及

b) 在与第三方共享的 IT 环境除外的情况下，并始终与供应商密切合作，对巴斯夫专用的基础设施、应用和服务开展安全测试，以发现并修复可能导致巴斯夫数据或信息遭受未经授权访问或披露风险的漏洞和薄弱环节；以及

c) 使巴斯夫能够满足适用网络安全法律，或确认供应商满足适用网络安全法律；

(2) 供应商应配合上述审计，且不向巴斯夫收取任何额外费用。

(3) 巴斯夫有权委托对第三方负有保密义务的合格外部审计师开展审计，但该审计师不得为供应商的竞争对手。本条不限制或排除巴斯夫依法享有的监督权和知情权。

(4) 所有审计和检查均应以只读方式进行，以确保数据或系统不会被更改、删除或篡改。

(5) 任何审计均应遵守适用法律，包括当地有关数据保护、网络安全、数据本地化、国家秘密、劳动用工及数据跨境传输的要求。供应商无需披露涉及其他客户的信息、受法律特权保护的信息、政府涉密信息、源代码（明确约定的除外）或适用法律禁止披露的信息。

6) 渗透测试

(1) 在本协议有效期内，巴斯夫有权随时对供应商的 IT 系统和 IT 网络开展高级模拟攻击（“渗透测试”）。该测试应仅由具备相应专业能力的独立第三方服务提供商或巴斯夫自身的网络安全专家（“渗透测试方”）执行。为确保渗透测试依照适用法律开展，双方将与渗透测试方签订三方协议，约定渗透测试的具体细节。供应

商仅可在有客观正当理由的情况下（例如渗透测试方和/或其任一关联公司为供应商的竞争对手）以书面形式拒绝聘用该渗透测试方。渗透测试通常在非生产环境中进行。

(2) 若供应商不允许巴斯夫开展渗透测试，则供应商应：

- 向巴斯夫提供由供应商或独立第三方开展的渗透测试的详细报告。
- 确保此类测试至少每十二（12）个月进行一次。
- 报告应包括：
    - 测试范围和方法
    - 已识别的漏洞及基于 CVSS 的风险评级
    - 已采取的整改措施
    - 已修复漏洞的验证情况

(3) 如渗透测试结果中包含 CVSS 评分达到 7 分或以上的发现项，供应商应立即启动整改措施，并允许开展复测以验证已识别问题的解决情况。

如供应商未能在第 4 节（供应商安全风险评估）规定的时限内充分修复已识别的漏洞，巴斯夫有权行使第 4 节第(4)款和第(5)款所述的权利。

7) 网络安全事件

供应商应制定并维护用于处理网络安全事件的书面事件响应计划，其中应包括：(i) 明确的角色与职责；(ii) 检测、遏制、根除和恢复程序；(iii) 证据收集与保全程序；(iv) 事后分析与经验总结流程；以及 (v) 实施适当纠正措施以防止再次发生的程序。

供应商还应确保在其组织内部提供多种信息安全事件报告渠道，并确保清晰的报告指引便于获取（例如通过内网）。

如供应商发现或获知网络安全事件，应：

a) 在不无故拖延的情况下通知巴斯夫，且无论如何应：(i) 对于涉及严重漏洞被利用、正在发生的数据外泄、勒索软件或可能触发监管报告义务的任何网络安全事件，在二十四（24）小时内通知；(ii) 对于任何其他网络安全事件，在七十二（72）小时内通知；通知方式为发送电子邮件至 third-party-breaches@basf.com，对于第(i)项下的事件，还应另行电话通知巴斯夫指定的联系人。初次通知应在当时已知的范围内包括：事件的性质和范围、受影响的系统和数据、影响的初步评估以及已采取的遏制措施；

b) 采取一切必要措施查明事实、控制损失，并协助巴斯夫开展上述工作；

c) 接受巴斯夫因网络安全事件为保护巴斯夫 IT 基础设施而采取的一切合理措施（例如断开 IT 系统连接或重置凭据）；

d) 确保与巴斯夫 IT 基础设施顺利重新连接；

e) 如信息安全事件导致本服务中断或延迟、运营效率下降或数据丢失，协助巴斯夫恢复数据；

f) 在事件解决前定期提供状态更新（在事件响应进行期间至少每日一次），并在事件关闭后十四（14）个自然日内提交最终事件报告；

g) 配合巴斯夫、监管机构或执法机关开展的任何调查，并在事件发生后至少十二（12）个月内保全所有相关证据。

8) 业务连续性管理

供应商应实施并维护符合 ISO 22301 或同等标准的业务连续性管理体系（BCMS），并应向巴斯夫提供其支持巴斯夫的服务所对应的业务连续性和灾难恢复计划的证明材料，包括至少每年一次的测试结果。BCMS 应包括：(i) 经与巴斯夫商定的、针对每个关键服务组件的恢复时间目标（RTO）和恢复点目标（RPO）；(ii) 书面的备份和恢复程序；(iii) 危机管理程序，包括升级路径和沟通计划；以及 (iv) 定期测试

和验证恢复程序（至少每年一次，关键服务应更频繁）。巴斯夫将继续负责其自身的业务连续性管理活动，并将事先审批供应商的灾难恢复相关活动。供应商应与巴斯夫密切合作，确保巴斯夫的业务连续性计划与供应商的业务连续性和灾难恢复计划妥善衔接。供应商应定期（至少每年一次）对所有巴斯夫应用开展业务影响分析，并据此确定适当的业务连续性要求。

9) 供应链安全

供应商应确保其参与提供本服务的所有分包商：(i) 在委托前接受书面安全评估；(ii) 通过适当的背对背合同安排，在合同上受约束遵守至少等同于本附件（网络安全）所含要求的安全要求；以及 (iii) 接受对其安全状况的持续监控和定期重新评估（至少每年一次）。该义务应沿整个供应链相应传递。供应商应维护所有可访问巴斯夫数据或巴斯夫 IT 系统的分包商名册，并应要求向巴斯夫提供该名册。如处理巴斯夫数据或可访问关键服务组件的分包商发生任何变更，供应商应至少提前三十（30）个自然日书面通知巴斯夫。

10) 人力资源安全与人员要求

供应商应实施并维护适当的人力资源安全措施，包括：(i) 在适用法律允许的范围内，并与数据和服务的敏感程度相适应，对所有可访问巴斯夫数据或巴斯夫 IT 系统的人员进行背景调查；(ii) 由所有相关人员签署保密承诺；(iii) 制定人员变动管理的书面程序，包括在影响关键服务交付或安全岗位的人员发生变动时及时通知巴斯夫；以及 (iv) 对违反信息安全政策的行为执行纪律处分程序。

11) 客户协作

巴斯夫应本着诚信原则与供应商合作，以协助供应商履行本附件项下的义务，包括：(i) 及时向供应商提供有关巴斯夫 IT 环境、安全要求和风险评估的必要信息；(ii) 在开展安全相关活动所需的范围内，向供应商提供对巴斯夫系统和人员的合理访问；(iii) 及时通知供应商可能影响本服务的、涉及巴斯夫系统的任何安全事件或漏洞；以及 (iv) 及时就安全报告、评估及拟议整改措施提供反馈。

II. **软件相关特别规定**

1) 产品与软件网络安全要求

(1) 如本服务包括开发、许可、供应、实施、维护或支持软件或带有数字元素的产品，供应商应在此类软件或产品的整个生命周期内实施并维持适当的网络安全措施。

供应商应确保软件或产品的设计、开发、配置和维护遵循“设计即安全”和“默认即安全”原则，并考虑其预期用途、可合理预见的误用、暴露程度、技术架构、所处理的数据、资产关键性以及对巴斯夫的潜在影响。

软件或产品在交付或发布时，不得包含任何未经适当修复、缓解、经巴斯夫正式接受风险，或未通过双方书面约定的整改计划予以处理的已知可利用漏洞。

(2) 供应商应向巴斯夫提供安全部署和使用软件或产品所合理必需的安全信息，在适用情况下包括：

a) 安全安装、配置和运行说明；

b) 身份认证和访问控制要求；

c) 相关安全假设、依赖关系及已知限制；

d) 受支持的版本及安全更新程序；

e) 已公布的支持终止日期或支持政策；以及

f) 安全停用、数据归还和数据删除说明。

此类信息的范围和详细程度应与软件或产品的性质、预期用途和网络安全风险相适应。

(3) 供应商应制定并维护协调漏洞披露政策，并在获知根据本协议供应的任何产品或软件存在漏洞时，在不无故拖延的情况下通知巴斯夫；且无论如何，对于正被积极利用的漏洞，应在发现后二十四（24）小时内通知；对于可能影响巴斯夫的任何其他漏洞，应在发现后七十二（72）小时内通知。

(4) 供应商应确保为巴斯夫开发或向巴斯夫供应的所有软件符合当前适用技术标准中规定的要求，包括 ISO/IEC 27001、ISO/IEC 27034、ISO/IEC 5230、ISO/IEC 18974、OWASP 应用安全验证标准（ASVS

）、OWASP 软件保障成熟度模型（SAMM）、NIST 安全软件开发框架（SSDF）、CycloneDX、SPDX。适用技术标准的选择应由双方根据软件的性质和关键程度商定。

(5) 如供应商为巴斯夫开发、修改或维护源代码，供应商应制定并应用安全编码原则的书面规范，并在编码前、编码中和编码后开展与风险相适应的安全检查。应建立强制性代码审查流程，并对源代码版本进行集中管控。此外，源代码和开发工具的访问权限应仅限于经授权人员，编辑权限仅授予指定人员，并应部署源代码管理系统以确保完整性和可追溯性。

(6) 供应商应自首次交付之日起至少五（5）年内，或在适用网络安全法律针对适用产品类别要求的更长期限内，为根据本协议供应的任何软件提供安全更新和补丁。在该支持期内，供应商应：(i) 免费提供用于修复已识别漏洞的安全更新；(ii) 至少提前十二（12）个月向巴斯夫通知支持终止日期；以及 (iii) 如技术上无法继续提供支持，提供迁移支持或替代解决方案。

2) SBoM 的编制

(1) 此外，供应商应负责针对交付给巴斯夫的每一个软件版本，以行业最佳实践格式（如 CycloneDX、软件包数据交换格式（SPDX）或 SWID 标签）并遵循适用技术标准，提供一份机器可处理的文件，列明软件中使用的所有组件（包括自有、第三方、专有及开源组件）的明细清单（以下简称“软件物料清单”或“SBoM”）。

(2) SBoM 至少应包含技术标准中规定的必填数据字段，包括但不限于：

a) SBoM 的创建者

b) SBoM 数据编制的时间戳

c) 组件创建者、（文件）名称及版本

d) 对其他组件的依赖关系

e) 相关许可证

f) 可部署组件的哈希值

g) 可执行、归档及结构化属性

3) SBoM 的交付与维护

在本协议有效期内，供应商应：

a) 确保 SBoM 始终完整、及时更新，并与约定的规格和要求保持一致；

b) 及时以书面形式（电子邮件即可）将 SBoM 的任何变更或更新告知巴斯夫；

c) 维护与 SBoM 相关的适当文档和记录；

d) 应巴斯夫要求，允许巴斯夫查阅上述记录及任何支持性文件，以核实 SBoM 的准确性和完整性；

e) 采取一切必要的纠正措施，纠正 SBoM 中的任何不准确、遗漏或不一致之处，并立即告知巴斯夫。

4) 安全测试/漏洞扫描

(1) 供应商有义务定期使用下列应用安全测试工具对软件的二进制代码和/或源代码进行分析，并应要求向巴斯夫提供此类漏洞扫描结果：

a) SCA = 软件成分分析

b) SAST = 静态应用安全测试

c) DAST = 动态应用安全测试

d) 人工渗透测试

e) （容器）漏洞扫描

f) 密钥/凭据泄露扫描（Secret Scanning）

(2) 如出现安全缺陷（例如软件组件存在恶意/易受攻击的行为），巴斯夫有权对该软件开展取证调查。

(3) 如存在易受攻击和/或恶意代码，供应商应在以下时限内修复代码并交付针对该漏洞的安全修复：(i) 严重漏洞：七十二（72）小时内；(ii) 高危漏洞：三十（30）个自然日内；(iii) 其他漏洞：按照双方商定的整改时间表执行。这明确包括以合规模块替换不合规的第三方模块（专有及开源）的义务，或对所有已发现漏洞进行技术修复的义务。在此情况下，具有以下特征的软件模块被视为不合规：已停止维护、包含 CVSS 评分 7.0 或以上的未修补漏洞，或已无法获得安全热修复。

5) 安全开发生命周期

(1) 供应商应实施并维护安全软件开发生命周期（SDLC），将安全融入软件开发的各个阶段，包括需求、设计、实施、测试、部署和维护。SDLC 应包括：

a) 在设计阶段开展威胁建模和安全架构评审；

b) 遵循安全编码标准（如 OWASP 安全编码实践、CERT 安全编码标准）；

c) 在代码合并至生产分支前，开展以安全为重点的强制性同行代码评审；

d) 在 CI/CD 流水线中集成自动化安全测试，包括 SAST、DAST、SCA 和密钥扫描；

e) 发布前开展安全验收测试；

f) 制定安全构建、发布和部署流程的书面程序。

变更历史

日期	作者	版本	备注
24.11.2025	Julia Mansky & Sebastian Nardone	1.0	初始文件 （本文件系在供应商安全相关监管变化和更新后首次编制。）
25.02.2026	Julia Mansky & Sebastian Nardone	1.1	监管变化： 1) 欧洲议会法规（EU）2024/2847 2) ISO 27001:2022 拼写错误更正
23.11.2026	Julia Mansky & Sebastian Nardone	1.2	1) 修订并进一步细化了多个主题领域 2) 新增定义 3) 引入改进供应链安全的变更 4) 修订 CRA 章节 5) 新增第 10 章“人力资源安全与人员要求”和第 11 章“客户协作”