附件 XY

非 IT 网络安全补充协议

版本 1.1

日期：23.11.2026

定义

就本《非 IT 网络安全附录》而言，下列术语具有如下含义：

“适用的网络安全法律”是指对任何一方、服务、相关产品、处理活动，或服务提供、接收、托管、运营、访问、分发或投放市场所在地区具有约束力的所有网络安全、信息安全、产品安全、关键信息基础设施安全、网络事件报告及其他相关法律、法规、监管要求和强制性标准。

仅在相关具体情形确有适用的范围内，此类法律可包括《NIS2 指令》（欧盟）2022/2555 及其各成员国实施法规、德国 BSIG、《欧盟条例》2022/2554（“DORA”）、《欧盟条例》2024/2847（“CRA”），以及相关亚太司法管辖区适用的网络安全法律法规；上述法律法规均包括其不时修订或替代的版本。

本附录对任何法律的引用，本身不应被解释为对该法律适用于供应商、服务或某项特定交易的陈述或确认。

“网络安全事件”是指对以下事项已经造成或可能造成重大不利影响的任何事件或一系列事件：(i) 服务、BASF 数据或 BASF IT 系统的机密性、完整性或可用性；或 (ii) 用于提供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，或任何其他导致技术和组织措施（ToMs）受损的情形。

I. IT 安全通用规定

1. 各方均应遵守在相关司法管辖区内对该方、服务或相关产品具有约束力的适用网络安全法律。因此，即使供应商并不提供 IT 服务，供应商仍应至少在其自身组织内实施并持续维护与合同履行相关的适当技术和组织措施、内部控制及信息安全管理机制（以下简称“ToMs”），以保护供应商自身网络和信息系统的完整性与韧性。此类 ToMs 应包括但不限于：
   a. 建立网络安全事件处置流程，包括网络安全事件响应计划等措施；
   b. 定期为所有供应商人员开展网络安全意识培训（每个自然年至少一次）；
   c. 建立流程，以确保网络和信息系统在采购、开发及维护过程中的网络安全，并定期对供应商的系统和解决方案开展漏洞扫描；对识别出的漏洞，应在合理可行的情况下尽快修补或采取缓解措施；
   d. 建立定期评估 ToMs 有效性的程序，例如开展内部审查；
   e. 如供应商存储或传输 BASF 的机密信息，应采用适当的加密措施；
   g. 如供应商以实体形式存储 BASF 的机密信息，应采取适当的物理安全措施（例如上锁存放和访问控制）；
   h. 实施多因素身份验证。

   供应商可通过取得并持续保持有效的行业标准框架认证（例如 ISO/IEC 27001），或应 BASF 要求提供其 ToMs 的合理证明文件，以证明符合上述要求。

2. 除上述最低要求外，如已事先获知 BASF 的相关安全政策，供应商在进入 BASF 场所或设施时还应遵守该等政策。对于供应商自身与合同履行相关的政策，如其政策发生可能对合同履行安全产生重大影响的变更，供应商应提前给予 BASF 合理通知。
3. 如 BASF 数据包含个人数据，实施并遵守上述措施以及合同文件规定的任何附加安全措施，旨在为 BASF 个人数据的处理提供适当的安全水平，并且在任何时候均应符合适用的数据保护法律法规。
4. **网络安全事件**

   如供应商发现或知悉网络安全事件，应：

   a. 在不无故延迟的情况下通知 BASF，且无论如何应满足以下时限：(i) 对于涉及严重漏洞、正在进行的数据外泄、勒索软件，或可能触发监管报告义务的任何网络安全事件，应在二十四

（24）小时内通知；(ii) 对于其他网络安全事件，应在七十二（72）小时内通过电子邮件通知 third-party-breaches@basf.com；对于第 (i) 项所述事件，还应通过电话通知 BASF 指定的联系人。初次通知应在当时已知的范围内包括：事件的性质及范围、受影响的系统和数据、初步影响评估以及已采取的遏制措施。供应商还应采取一切必要措施查明事实、限制损害，并协助 BASF 开展相关工作；

c. 接受 BASF 因网络安全事件而采取的、旨在保护 BASF IT 基础设施的所有合理措施（例如断开 IT 系统连接或重置凭据）；

f. 应 BASF 要求，就网络安全事件提供书面报告，包括事件的性质和范围、已采取的措施以及防止再次发生的措施。

5. 供应链安全

供应商应确保参与合同履行的分包商通过合同承担至少与本附录所载网络安全要求同等的义务，并确保该等义务沿供应链相应向下传递。

6. 变更历史

日期	作者	版本	备注
24.11.2025	Sebastian Nardone & Julia Mansky	1.0	初始版本 （本文件最初是在法规变更及供应商安全要求更新后制定。）
23.11.2026	Sebastian Nardone & Julia Mansky	1.1	对内容进行了重新表述和简化，以更好地满足中小型企业的实际需求。