BASF Group –
Cyber Security Addendum

版本	5.1
分类	PUBLIC

版本详细信息

版本	5.1
创建者	Sebastian Krüsmann, NeoMINT GmbH
现状	批准
批准日期	10.01.2024
批准人	Julia Mansky，巴斯夫数字解决方案有限公司
更新在	Download Center (basf.com)

历史

版本	日期	创建者	变化
1.0	02.10.2023	Sebastian Krüsmann, NeoMINT GmbH	初始创建
2.0	09.10.2023	Sebastian Krüsmann, NeoMINT GmbH	编辑改动
3.0	17.10.2023	Sebastian Krüsmann, NeoMINT GmbH	编辑改动
4.0	21.11.2023	Sebastian Krüsmann, NeoMINT GmbH	编辑改动
5.0	08.01.2024	Sebastian Krüsmann, NeoMINT GmbH	编辑改动
5.1	08.08.2024	Beatrice Huck, NeoMint GmbH	增加对照 C-T-12 和 S-T-12、CL-T-15 C-T-13 和 S-T-13、CL-T-16、CL-T-09、C-T-06 和 S-T-06 控制权变更 CL-T-16, CL-T-09, C-T-06 和 S-T-06

目录

1 免责声明

安全增补件包含信息安全要求。

所有 IT 供应商都必须满足 "一般 "一章中的规格要求。**其他要求按供应商类型分列**，并应相应满足。有关供应商类型的说明，请参见相应章节的开头部分。

针对每种供应商类型，都有章节介绍具体风险以及应对风险所要达到的目标。为此，通常可以采取各种技术性或组织性措施。如果风险与具体情况无关，或者供应商认为可以采用与所述不同的方式来应对风险，则可以对此进行简要说明。巴斯夫可自行决定所给出的理由和措施是否充分。

2 网络安全联络点

为了确保与我们的 IT 供应商进行无缝、高效的合作，以保持适当的网络安全水平，每个供应商都必须指定网络安全核心角色的联系人和联系信息。

内部客户（iBP 或采购部）将信息记录在表格 *2 IT 供应商安全评估_EN_联系表中*，以当前版本的德语或英语提供给每个供应商，并发送给供应商安全团队。

3 一般情况

如果无论提供何种服务都存在风险，则一般供应商安全就具有相关性。

3.1 (网络安全/信息安全（单一）联络点 (SPoC)

与供应商在网络安全问题上的沟通不足或延迟，可能导致漏洞处理不及时或不充分。

目标 有关网络安全问题的查询，例如有关已实施的安全措施或发现影响供应商的安全事件的查询，将在合理的时间内得到答复。

技术措施	
G-T-01	提交查询并及时回复的平台，如票据系统

组织措施	
G-O-01	网络安全问题联络人，如 CISO/信息安全官

3.2 人力资源安全

应对风险 供应商的员工可能会有意或无意地通过他们的行为对巴斯夫的安全水平产生重大的负面影响。

目标 只有具备足够资格和意识的员工才有权访问巴斯夫的信息或系统。

技术措施	
G-T-02	角色和授权概念：员工只能访问与其工作相关的信息（"需要知道 "原则）
组织措施	
G-O-02	定期对所有员工进行网络安全意识培训

3.3 信息安全管理

应对风险 网络安全的概念化和可操作性不足，可能导致无法在早期阶段识别或避免漏洞。攻击者利用这些漏洞可能会对巴斯夫的安全水平产生负面影响。

目标 积极主动地设计和管理供应商的整个安全机制。

组织措施	
G-O-03	指定专人负责维护适当水平的网络安全，如 CISO 或信息安全官
G-O-04	在信息安全管理系统（ISMS）范围内对所有网络安全措施进行全面管理
G-O-05	基于既定标准（如 ISO 27001）的信息安全管理系统认证

3.4 供应链安全

应对风险 网络安全的概念化和可操作性不足，可能导致无法在早期阶段识别或避免漏洞。攻击者利用这些漏洞可能会对巴斯夫的安全水平产生负面影响。

目标 要求所有材料分包商和供应商建立并维持适当水平的网络安全。

组织措施	
G-O-06	为巴斯夫提供服务的次级供应商登记册
G-O-07	分包商和供应商有合同义务建立和维护适当水平的网络安全

3.5 变革管理

应对风险 对所提供服务和产品的变更控制不力，可能导致信息丢失和性能下降，从而对巴斯夫的运营产生负面影响。

目标 建立标准化和正规化的程序，以协调和承诺所提供服务和产品的变更。

技术措施	
G-T-03	管理和记录所有合同和服务变更的平台

组织措施	
G-O-08	(合同服务变更的（单一）联络点 (SPoC)

3.6 合规性

应对巴斯夫可能因供应商违反法律法规而承担责任的**风险**。

目标 始终遵守所有适用的合规要求。

组织措施	
G-O-09	指定专人负责维护全球合规性，如合规官
G-O-10	在合规管理系统（CMS）范围内管理所有合规措施

4 咨询服务

与组织发展以及信息技术解决方案的提供、运行或退役直接或间接相关的所有咨询服务。

4.1 资源管理

应对风险 工作人员短缺可能导致无法提供合同商定的服务。

目标 保证在任何时候都有足够合格的员工来提供合同约定的服务。所有服务都能按时按质交付。

组织措施	
C-O-01	在内部资源管理范围内管理人力资源，提供合格的人员
C-O-02	专家和管理人员的培训与发展理念

4.2 信息处理

解决的风险 咨询项目中使用的信息如果失去保密性，可能会危及巴斯夫的网络安全。

目标 始终确保在咨询项目范围内创建和接收的所有信息都得到保密处理，并防止外泄。

技术措施	
C-T-01	使用既定的行业标准（如 PGP、S/MIME）对电子邮件通信进行加密
C-T-02	移动设备硬盘加密，如 BitLocker、Vera Crypt
C-T-03	服务器硬盘加密，如 BitLocker、Vera Crypt
C-T-04	移动数据载体加密，例如 BitLocker、Vera Crypt、硬件加密

C-T-05	管理端到端身份和访问管理（IAM）范围内的所有权限

组织措施

C-O-03	在项目之前、期间和之后存储、处理和发送信息的政策
C-O-04	安全事件处理流程
C-O-05	移动设备丢失时的远程数据抹除程序
C-O-06	确保只有为巴斯夫提供咨询服务的员工才能访问巴斯夫信息的流程（"需要知道 "原则）
C-O-07	当员工加入或离开公司或改变角色时，授予、更改或撤销访问权限的流程（加入者-流动者-离开者流程）
C-O-08	根据重要程度对处理过的信息进行分类的概念

4.3 恶意软件保护

应对风险 如果咨询过程中使用的 IT 设备遭到破坏，信息可能会被无意更改或被未经授权的第三方获取。

目标 确保 IT 设备上不会安装恶意软件。

技术措施	
C-T-06	Windows 服务器恶意软件保护解决方案
C-T-07	客户端的恶意软件保护解决方案，如 Microsoft Defender
C-T-08	安全设备，如防火墙、SIEM
C-T-09	根据所处理数据的保密性和可用性要求的关键性，对企业网络进行适当划分
C-T-10	使用沙箱解决方案打开未知文件或来自未知发件人的文件。
C-T-11	集中管理的软件分发
C-T-12	不授予开发商地方行政权
C-T-13	不授予普通用户本地管理权限
组织措施	
C-O-09	对所有使用中的软件解决方案立即安装与安全相关的更新程序
C-O-10	服务器加固政策
C-O-11	客户加固政策

C-O-12　　智能手机的加固政策

4.4 数据备份

应对风险 系统错误、恶意软件或滥用 IT 系统可能导致咨询项目范围内收集的数据丢失。

目标 定期备份与巴斯夫有关的所有数据，并可在数据丢失时进行恢复。

技术措施	
C-T-14	定期自动备份与巴斯夫有关的所有数据
组织措施	
C-O-13	数据备份概念
C-O-14	定期进行数据备份和恢复练习

4.5 实体安全

应对风险 在供应商处所处理时，巴斯夫的信息可能会被外部人员泄露。

目标 来自巴斯夫或与巴斯夫有关的所有信息都受到保护，防止未经授权的第三方进行实际访问。

技术措施	
C-T-15	带锁办公室
C-T-16	带锁的柜子或保险箱
组织措施	
C-O-15	员工在供应商物业内陪同客人的政策

C-O-16 锁定数据存储介质、IT 设备和文件的政策

4.6 保护个人身份信息（PII）

应对风险 在合同处理范围内处理 PII 时，信息的不当使用可能会损害数据主体的个人权利。

目标 在处理 PII 时，始终确保遵守 GDPR 和下游数据保护法规的要求。

组织措施	
C-O-17	指定数据保护负责人，如数据保护官
C-O-18	在数据保护管理系统（DMS）范围内保护所有个人身份信息的整体性

5 服务与支持

管理、维护或处置解决方案范围内的所有服务和支持服务。这涵盖了解决方案的整个产品生命周期，从安装开始到处置结束。

5.1 资源管理

应对风险 工作人员短缺可能导致无法提供合同商定的服务。

目标 保证在任何时候都有足够合格的员工来提供合同约定的服务。所有服务都能按时按质交付。

组织措施	
S-O-01	在内部资源管理范围内管理人力资源，提供合格的人员
S-O-02	专家和管理人员的培训与发展理念

5.2 信息处理

解决的风险 在服务和支持任务中使用的信息如果失去保密性，可能会危及巴斯夫的网络安全。

目标 始终确保在服务和支持活动范围内创建和接收的所有信息都得到保密处理，并防止泄密。

技术措施	
S-T-01	使用既定的行业标准（如 PGP、S/MIME）对电子邮件通信进行加密
S-T-02	移动设备硬盘加密，如 BitLocker、Vera Crypt
S-T-03	服务器硬盘加密，如 BitLocker、Vera Crypt
S-T-04	移动数据载体加密，例如 BitLocker、Vera Crypt、硬件加密
S-T-05	管理端到端身份和访问管理（IAM）范围内的所有权限
组织措施	
S-O-03	在任务之前、期间和之后存储、处理和发送信息的政策
S-O-04	**安全事件处理流程**
S-O-05	移动设备丢失时的远程数据抹除程序
S-O-06	确保只有为巴斯夫提供咨询服务的员工才能访问巴斯夫信息的流程（"有必要知道 "原则）
S-O-07	当员工加入或离开公司或改变角色时，授予、更改或撤销访问权限的流程（加入者-流动者-离开者流程）
S-O-08	根据重要程度对处理过的信息进行分类的概念

5.3 恶意软件保护

应对风险 如果在服务和支持任务中使用的 IT 设备遭到破坏，信息可能会被无意更改或被未经授权的第三方获取。

目标 确保 IT 设备上不会安装恶意软件。

技术措施	
S-T-06	Windows 服务器恶意软件保护解决方案
S-T-07	客户端的恶意软件保护解决方案，如 Microsoft Defender
S-T-08	安全设备，如防火墙、SIEM
S-T-09	根据所处理数据的保密性和可用性要求的关键性，对企业网络进行适当划分
S-T-10	使用沙箱解决方案打开未知文件或来自未知发件人的文件。
S-T-11	集中管理的软件分发
S-T-12	不授予开发商地方行政权
S-T-13	不授予普通用户本地管理权限
组织措施	
S-O-09	对所有使用中的软件解决方案立即安装与安全相关的更新程序
S-O-10	服务器加固政策
S-O-11	客户加固政策

S-O-12　　智能手机的加固政策

5.4 数据备份

应对风险 系统错误、恶意软件或滥用 IT 系统可能导致丢失与巴斯夫有关的数据。

目标 定期备份与巴斯夫有关的所有数据，并可在数据丢失时进行恢复。

技术措施	
S-T-14	定期自动备份与巴斯夫有关的所有数据
组织措施	
S-O-13	数据备份概念
S-O-14	定期进行数据备份和恢复练习

5.5 实体安全

应对风险 在供应商处所处理时，巴斯夫的信息可能会被外部人员泄露。

目标 来自巴斯夫或与巴斯夫有关的所有信息都受到保护，防止未经授权的第三方进行实际访问。

技术措施	
S-T-15	带锁办公室
S-T-16	带锁的柜子或保险箱
组织措施	
S-O-15	员工在供应商物业内陪同客人的政策

S-O-16　锁定数据存储介质、IT 设备和文件的政策

5.6 保护个人身份信息（PII）

应对风险 在合同处理范围内处理 PII 时，信息的不当使用可能会损害数据主体的个人权利。

目标 在处理 PII 时，始终确保遵守 GDPR 和下游数据保护法规的要求。

组织措施	
S-O-17	指定数据保护负责人，如数据保护官
S-O-18	在数据保护管理系统（DMS）范围内保护所有个人身份信息的整体性

5.7 远程访问

解决的风险 远程访问会话可能被未经授权的人员用作进入巴斯夫网络的网关。不安全的协议、配置、密码和应用程序可能允许未经授权的访问。

目标 在任何远程访问过程中，都要确保对存储、处理和传输的信息和数据的保护，以及巴斯夫基础设施的完整性。

技术措施	
S-T-17	在访问巴斯夫数据和基础设施时使用安全协议、加密方法和应用程序
组织措施	
S-O-19	所有远程访问会话的完整文档或记录

5.8 信息技术管理

应对风险 IT 管理不当可能导致巴斯夫的基础设施中断或受损。

目标 所有服务和支持活动均按照安全管理的行业最佳做法进行。

技术措施	
S-T-18	管理服务和支持请求的票单系统
组织措施	
S-O-20	管理和记录服务和支持人员使用的工具
S-O-21	立即为所有使用的软件解决方案安装与安全相关的更新和修补程序
S-O-22	开展服务和支持活动的流程。

6 硬件组件

采购安装在终端上或需要终端使用的单个硬件组件，如鼠标、键盘、屏幕、内存、硬盘等。

6.1 送货

应对风险 硬件组件可能在交付过程中损坏。此外，组件还可能被篡改，从而危及巴斯夫的基础设施。

目标 所有硬件组件功能齐全，以整数状态按预定配置交付。

技术措施	
H-T-01	接收、处理和解决投诉和退货的平台
H-O-01	确保每批货物在装运前完整无缺的流程
组织措施	
H-O-02	实时货物跟踪
H-O-03	保护货物不受损坏
H-O-04	密封所有货物

6.2 产品安全

解决的风险 不合适、损坏或被篡改的组件可能导致巴斯夫基础设施中断或受损。

目标 所有硬件组件均由供应商或上游供应商进行功能和完整性测试。为所有硬件组件提供充足的技术文档，以便为特定应用选择最佳组件。

组织措施

H-O-05	记录所有组件的理想运行环境
H-O-06	供应商或上游供应商验证所有组件功能和完整性的流程

7 终端与设备

采购计划供最终用户或数据中心使用的设备，如笔记本电脑、智能手机、服务器等，以及设备（单用途设备/具有专门操作系统的设备，是运行所必需的），如防火墙、VPN 网关、路由器或交换机。

7.1 送货

应对风险 设备可能在交付过程中损坏。此外，组件可能会被篡改，从而危及巴斯夫的基础设施。

目标 所有物证均以整数状态按预定配置交付，功能齐全。

技术措施	
E-T-01	接收、处理和解决投诉和退货的平台
组织措施	
E-O-01	确保每批货物在装运前完整无缺的流程
E-O-02	实时货物跟踪
E-O-03	保护货物不受损坏
E-O-04	密封所有货物

7.2 产品安全

解决的风险 不合适、损坏或被篡改的设备可能导致巴斯夫基础设施中断或受损。

目标 所有设备均由供应商或上游供应商进行功能和完整性测试。为所有硬件组件提供充足的技术文档，以便为特定应用选择最佳组件。

组织措施	
E-O-05	记录所有组件的理想运行环境
E-O-06	供应商或上游供应商验证所有组件功能和完整性的流程

7.3 设备设置

解决的风险 当设备由供应商进行初始设置时，使用常见的、因此很容易猜到的默认配置可能会让攻击者入侵巴斯夫。

目标 在所有设备上安装安装时可用的安全相关更新和补丁。初始密码配置为用户必须在首次登录时更改。

组织措施	
E-O-07	安装操作系统和固件的所有可用更新和修补程序
E-O-08	使用初始密码，首次使用设备时必须更改密码
E-O-09	避免安装非必要的软件包，例如可选的 OEM 软件

8 企业内部解决方案

采购在巴斯夫基础设施（如笔记本电脑、服务器或智能手机）上运行的应用程序（软件包），使用时无需访问制造商的系统。

8.1 IT 安全概念

应对风险 如果在规划和开发过程中没有考虑到行业标准安全机制，或者没有认识到措施之间的相互作用，攻击者就可能利用由此产生的安全漏洞，破坏巴斯夫的信息、数据和基础设施。

目标 在 IT 安全概念的范围内定义解决方案的所有安全措施，并持续记录和更新变更后的实施状态。

组织措施	
O-O-01	为解决方案制定 IT 安全概念
O-O-02	定期更新信息技术安全概念，并在发生变化时进行更新
O-O-03	向巴斯夫提供已实施安全机制的文件

8.2 加密技术

应对风险 如果数据在存储、处理或传输过程中没有得到保护，就可能被未经授权的第三方截获或泄露。

目标 在整个生命周期内，保护数据免遭未经授权的访问。

技术措施	
O-T-01	传输过程中的数据加密（传输中的数据），如 HTTPS、SSH

O-T-02	存储过程中的数据加密，如数据库加密
O-T-03	多因素身份验证，以便访问敏感信息
O-T-04	对配置更改进行多因素验证

组织措施

O-O-04	加密概念，包括所有已实施的加密方法和密钥长度

8.3 角色和权限概念

解决的风险 角色和权限概念的缺失或不足会使未经授权的用户获取敏感信息。

目标 可以对角色和权限进行细化管理，使用户只能访问执行任务所需的信息。

技术措施

O-T-05	活动目录 API
O-T-06	LDAP API
O-T-07	完全通过分配角色来分配权限
O-T-08	用于角色和权限管理的软件模块/组件/功能

组织措施

O-O-05	正式记录角色和权限概念

8.4 更新和补丁

解决风险 如果与安全相关的更新和补丁发布后没有立即安装，攻击者可能会重建更新或补丁所解决的漏洞，并积极利用它。

目标 从更新和补丁发布到提供给巴斯夫，再到安装的时间非常短，攻击者不可能主动利用尚未修复的已知漏洞。

技术措施	
O-T-09	在解决方案中提供与安全相关的更新和补丁
O-T-10	通过供应商网站提供与安全相关的更新和补丁程序

组织措施	
O-O-06	通过电子邮件发送新发布的更新和补丁信息
O-O-07	有关解决方案中最新发布的更新和补丁的信息
O-O-08	通过供应商网站了解最新发布的更新和补丁信息

8.5 渗透测试

解决风险 解决方案的复杂性可能会导致由于子组件之间的相互作用及其产生的影响而使漏洞不被注意。攻击者可能会利用这些盲点。

目标 考虑到所有已知的攻击方法，定期审查整体解决方案的保护级别，并根据审查结果进一步开发。

组织措施	
O-O-09	定期对解决方案进行渗透测试
O-O-10	对解决方案进行事件驱动的渗透测试，例如在发生重大变更时
O-O-11	定期对第三方组件（如外部开发人员提供的软件模块）进行渗透测试

O-O-12	对第三方组件进行事件驱动的渗透测试，例如在发现安全漏洞或安全事件时进行测试

8.6 为用户提供支持和文档

解决的风险 用户手册缺失或不可用可能导致用户不使用或错误使用解决方案。这可能会对巴斯夫的运营产生不利影响。

目标 所有用户组都能以预期方式使用解决方案，达到预期目的。

技术措施	
O-T-11	供用户交流的社区论坛
O-T-12	用户服务台网站
O-T-13	用户热线电话
O-T-14	通过电子邮件为用户提供支持
组织措施	
O-O-13	由供应商自己的培训师为用户（团体）提供培训
O-O-14	由外部培训机构（如行业协会、TÜV（德国技术检验协会））向用户（团体）提供培训
O-O-15	为用户（群体）提供自学材料，如教程视频、演示文稿、分步骤说明等
O-O-16	一般用户手册
O-O-17	基于情景的用户手册

8.7 为管理员提供支持和文档

解决的风险 安装、分发或配置不当可能导致数据泄露或解决方案失效，从而中断巴斯夫的运营。

目标 负责操作解决方案的 BASF 管理员能够按照预期管理解决方案。

技术措施

O-T-15	供管理员交流的社区论坛
O-T-16	管理员服务台网站
O-T-17	管理员电话热线
O-T-18	通过电子邮件为管理员提供支持

组织措施

O-O-18	由供应商自己的培训师为管理员提供培训
O-O-19	由外部培训机构（如行业协会、TÜV（技术检验机构））为管理人员提供培训
O-O-20	供管理员使用的自学材料，如教程视频、演示文稿、分步骤说明等
O-O-21	一般管理员手册
O-O-22	基于情景的管理员手册

8.8 软件架构

解决的风险 如果允许从巴斯夫基础设施外部通过互联网访问，攻击者可能会利用功能和架构漏洞检索数据，或者在攻击成功的情况下，通过权限升级访问巴斯夫基础设施内的其他系统。

目标 数据处理的架构和流程都旨在保护解决方案和处理过的数据免遭未经授权的访问，并确保在个别组件受到破坏时不会影响巴斯夫的其他系统。

技术措施	
O-T-19	三层架构：将表现层、处理层和数据存储层分离开来
O-T-20	2 层架构：应用层和数据存储层分离
O-T-21	防止跨站点脚本攻击
O-T-22	输入验证，防止未经授权的数据操作，例如通过 SQL 注入进行数据操作

组织措施	
O-O-23	解决方案架构文档

9 云计算解决方案

采购在服务提供商基础设施上运行的应用程序（软件包），其使用要求必须接入互联网。至于解决方案是 SaaS（软件即服务）、PaaS（平台即服务）、Iaas（基础设施即服务）还是云技术，在此不作具体说明。

9.1 IT 安全概念

应对风险 如果在规划和开发过程中没有考虑行业标准的安全机制，或者没有确定措施之间的相互作用，攻击者就可能利用由此产生的漏洞，破坏巴斯夫的信息、数据和基础设施。

目标 在 IT 安全概念的范围内定义解决方案的所有安全措施，并持续记录和更新变更后的实施状态。

组织措施	
CL-O-01	为解决方案制定 IT 安全概念
CL-O-02	定期更新信息技术安全概念，并在发生变化时进行更新
CL-O-03	向巴斯夫提供已实施安全机制的文件

9.2 加密技术

应对风险 如果数据在存储、处理或传输过程中没有得到保护，就可能被未经授权的第三方截获或泄露。

目标 在整个生命周期内，保护数据免遭未经授权的访问。

技术措施	
CL-T-01	传输过程中的数据加密（传输中的数据），如 HTTPS、SSH
CL-T-02	存储过程中的数据加密，如数据库加密
CL-T-03	多因素身份验证，以便访问敏感信息
CL-T-04	对配置更改进行多因素验证
组织措施	
CL-O-04	加密概念，包括所有已实施的加密方法和密钥长度

9.3 角色和权限概念

解决的风险 角色和权限概念的缺失或不足会使未经授权的用户获取敏感信息。

目标 可以对角色和权限进行细化管理，使用户只能访问执行任务所需的信息。

技术措施	
CL-T-05	活动目录 API
CL-T-06	LDAP API

CL-T-07	完全通过分配角色来分配权限
CL-T-08	用于角色和权限管理的软件模块/组件/功能

组织措施

CL-O-05	正式记录角色和权限概念

9.4 恶意软件保护

应对风险 如果系统遭到破坏，信息可能会被无意更改或被未经授权的第三方获取。

目标 确保 IT 设备上不会安装恶意软件。

技术措施

CL-T-09	Windows 服务器恶意软件保护解决方案
CL-T-10	客户端的恶意软件保护解决方案，如 Microsoft Defender
CL-T-11	安全设备，如防火墙、SIEM
CL-T-12	根据所处理数据的保密性和可用性要求的关键性，对企业网络进行适当划分
CL-T-13	使用沙箱解决方案打开未知文件或来自未知发件人的文件。
CL-T-14	集中管理的软件分发
CL-T-15	不授予开发商地方行政权
CL-T-16	不授予用户本地管理权限

组织措施

CL-O-06	对所有使用中的软件解决方案立即安装与安全相关的更新程序

CL-O-07	服务器加固政策
CL-O-08	客户加固政策
CL-O-09	智能手机的加固政策

9.5 数据备份

应对风险 系统错误、恶意软件或滥用 IT 系统可能导致数据丢失。

目标 定期备份与巴斯夫有关的所有数据，并可在数据丢失时进行恢复。

技术措施

CL-T-17	定期自动备份与巴斯夫有关的所有数据
CL-T-18	自动部署工作流程，如 CI/CD

组织措施

CL-O-10	数据备份概念
CL-O-11	定期进行数据备份和恢复练习
CL-O-12	在对运行解决方案所需的系统和应用程序进行重大更改之前，手动快照系统状态

9.6 渗透测试

解决风险 解决方案的复杂性可能会导致由于子组件之间的相互作用及其产生的影响而使漏洞不被注意。攻击者可能会利用这些盲点。

目标 考虑到所有已知的攻击方法，定期审查整体解决方案的保护水平，并根据审查结果进一 步开发。

组织措施	
CL-O-13	定期对解决方案进行渗透测试
CL-O-14	对解决方案进行事件驱动的渗透测试，例如在发生重大变更时
CL-O-15	定期对第三方组件（如外部开发人员提供的软件模块）进行渗透测试
CL-O-16	对第三方组件进行事件驱动的渗透测试，例如在发现安全漏洞或安全事件时进行测试

9.7 为用户提供支持和文档

解决的风险 用户手册缺失或不可用可能导致用户不使用或错误使用解决方案。这可能会对巴斯夫的运营产生不利影响。

目标 所有用户组都能以预期方式使用解决方案，达到预期目的。

技术措施	
CL-T-19	供用户交流的社区论坛
CL-T-20	用户服务台网站
CL-T-21	用户热线电话
CL-T-22	通过电子邮件为用户提供支持

组织措施	
CL-O-17	由供应商自己的培训师为用户（团体）提供培训
CL-O-18	由外部培训机构（如行业协会、TÜV（德国技术检验协会））向用户（团体）提供培训
CL-O-19	为用户（群体）提供自学材料，如教程视频、演示文稿、分步骤说明等
CL-O-20	一般用户手册
CL-O-21	基于情景的用户手册

9.8 为管理员提供支持和文档

解决的风险 安装、分发或配置不当可能导致数据泄露或解决方案失效，从而中断巴斯夫的运营。

目标 负责操作解决方案的 BASF 管理员能够按照预期管理解决方案。

技术措施	
CL-T-23	供管理员交流的社区论坛
CL-T-24	管理员服务台网站
CL-T-25	管理员电话热线
CL-T-26	通过电子邮件为管理员提供支持

组织措施	

CL-O-22	由供应商自己的培训师为管理员提供培训
CL-O-23	由外部培训机构（如行业协会、TÜV（技术检验机构））为管理人员提供培训
CL-O-24	供管理员使用的自学材料，如教程视频、演示文稿、分步骤说明等
CL-O-25	一般管理员手册
CL-O-26	基于情景的管理员手册

9.9 软件架构

已解决的风险 攻击者可利用软件架构中的漏洞检索数据，或在攻击成功的情况下，通过权限升级访问巴斯夫基础设施内的其他系统。

目标 软件架构的设计旨在保护解决方案和处理过的数据免遭未经授权的访问，并确保在个别组件遭到破坏时不会影响巴斯夫的其他系统。

技术措施

CL-T-27	三层架构：将表现层、处理层和数据存储层分离开来
CL-T-28	2 层架构：应用层和数据存储层分离
CL-T-29	防止跨站点脚本攻击
CL-T-30	输入验证，防止未经授权的数据操作，例如通过 SQL 注入进行数据操作

组织措施

CL-O-27	解决方案架构文档

9.10 业务连续性管理

应对风险 关键系统组件的故障或失灵会导致云解决方案的可用性损失。特别是在关键业务流程的情况下，即使是短暂的中断也会给巴斯夫带来巨大损失。

目标 确保在整个合同期内履行商定的服务水平协议（SLA）。

技术措施	
CL-T-31	应急数据中心

组织措施	
CL-O-28	指定应急管理负责人，如业连管干事、应急干事
CL-O-29	在业务连续性管理系统（BCMS）的范围内，对所有应急管理措施进行全面管理
CL-O-30	冗余概念

9.11 保护个人信息（PII）

应对风险 在合同处理范围内处理 PII 时，信息的不当使用可能会损害数据主体的个人权利。

目标 在处理 PII 时，始终确保遵守 GDPR 和下游数据保护法规的要求。

组织措施	
CL-O-31	指定数据保护负责人，如数据保护官
CL-O-32	在数据保护管理系统（DMS）范围内保护所有个人身份信息的整体性

9.12 实体安全

应对风险 如果云解决方案在不安全的数据中心运行，服务器和其他 IT 组件可能会被操纵、窃取或破坏。

目标 提供云计算解决方案所需的所有基础设施都在安全的数据中心运行。

技术措施	
CL-T-32	灭火和防火系统
CL-T-33	多个防火隔间
CL-T-34	危险警报系统
CL-T-35	视频监控系统
CL-T-36	自动监测基础设施
CL-T-37	将数据中心连接到全天候有人值守的中央控制站
CL-T-38	温度和湿度管理
CL-T-39	不间断电源
CL-T-40	浪涌保护装置
组织措施	
CL-O-33	防尘措施
CL-O-34	门禁控制概念

10 软件开发

开发独立使用或与其他解决方案集成使用的软件解决方案或组件。这也包括解决方案的定制。解决方案的配置不属于软件开发范畴。

应用注意事项：当供应商自行开发解决方案时，除服务类型 "内部部署解决方案 "和 "云解决方案 "外，还需满足软件开发要求。

10.1 开发过程

解决的风险　如果不采用安全软件开发的最佳实践，可能会导致安全漏洞，从而被攻击者利用。这既适用于源代码，也适用于所提供安装介质的配置。

目标　标准化和有管理的开发流程可确保封闭所用软件（软件包）中的所有已知漏洞，并在部署前以足够安全的方式配置安装介质。

技术措施
SW-T-01　自动部署工作流程，如 CI/CD

组织措施	
SW-O-01	正式的安全软件开发生命周期（SSDLC）
SW-O-02	管理和记录开发过程中使用的工具
SW-O-03	根据标准化测试用例测试解决方案的新版本
SW-O-04	进行单元测试
SW-O-05	进行负载测试
SW-O-06	坚持原则：安全源于设计
SW-O-07	坚持原则：默认安全
SW-O-08	坚持原则：设计隐私
SW-O-09	坚持原则：默认隐私

10.2 第三方软件

应对风险 在使用第三方软件组件（如外部开发人员提供的软件模块）时，这些组件中的漏洞可能成为攻击者未经授权访问数据的攻击载体。

目标 定期检查所有第三方软件组件是否存在漏洞。供应商通过为解决方案商定的一般更新和补丁渠道提供与安全相关的外部组件更新和补丁。

组织措施	
SW-O-10	注册所有第三方软件组件

SW-O-11　对使用中的第三方软件组件的已知漏洞进行定期测试。