信息安全计划

范畴：本信息安全计划（Information Security Plan 以下简称“ISP”）已纳入客户与 Infor 签订的各项协议中（统称“协议”）。若本 ISP 条款与协议中的任何其他条款存在冲突或不一致，应以本 ISP 条款为准。本 ISP 规定了 Infor 当前实施的安全措施，该等措施旨在为所有客户提供以下方面的总体保障：

- ⅰ. Infor 用于提供以下服务的硬件、设备及系统软件配置：

  a. 云服务（为明确起见，云服务包含支持服务）
  b. 专业服务，以及
  c. 本地部署软件相关支持服务
  （本 ISP 中，所有此类硬件、设备及系统软件配置统称为“系统”；云服务、专业服务及本地部署软件支持服务统称为“服务”）；

同时也保障

- ⅱ. 客户向 Infor 提供的数据，包括：

  a. 客户数据本身，或
  b. 客户为便于 Infor 在其自身环境中提供专业服务和/或支持服务而提供的数据
  （本 ISP 中，所有此类数据统称为“数据”）。

定义：本 ISP 中使用但未在本 ISP 内定义的术语，其含义以 Infor 与该客户签订的软件协议（以下简称“协议”）中赋予的含义为准。

除外情形：本 ISP 不适用于以下情况：(i) 根据单独协商的专业服务协议，Infor 为客户托管其本地部署软件的专业服务；(ii) Infor 在客户场所内提供服务和/或获得客户系统访问权限的情形。在前述情况下，Infor 应遵守工作说明书中双方约定的客户行政、技术及场所要求；就 Infor 访问客户系统相关事宜，客户负责向 Infor 人员提供系统访问所需的用户授权及密码，并根据自身判断适时撤销该等授权、或终止访问权限。

更新：由于安全威胁及防范该等威胁的措施始终处于不断演变之中，因此 Infor 可能随时需要修改本 ISP，且无需事先通知客户，但前提是 Infor 对系统和数据的总体安全保障水平维持不变或有所提升。

1. 一般安全标准

Infor 制定并维持一套管理、技术及物理保障措施，旨在防范系统和数据遭受破坏、丢失、未授权访问或篡改，该等措施需满足：(i) 不低于 Infor 为自身同类性质信息所采取的保障水平；(ii) 不低于行业公认标准；(iii) 符合适用法律的要求。Infor 对第三方操作系统以及与系统交互的以下产品和服务不承担任何责任：(a) 客户自行开发或委托他人为其开发的产品和服务；(b) 客户根据第三方自身适用许可条款授权使用的产品和服务。

1.1 安全官

Infor 已任命一名或多名安全官，负责协调和监督本 ISP 中各项安全措施的执行。

1.2 访问控制

Infor 对数据实施访问控制，包括但不限于以下措施：

ⅰ. Infor 为每一位有权通过计算机访问数据的人员分配唯一标识（ID）。

ii. Infor 明确有权授予、变更或撤销数据访问权限的人员，并基于最小权限原则限制数据访问。仅允许因提供服务而“有必要知晓”的数据相关人员访问数据，Infor 将留存并及时更新该等人员的记录，且对数据访问行为进行日志记录和监控。

iii. Infor 要求有权访问数据的 Infor 人员，在计算机无人值守时禁用管理会话。

iv. 当 Infor 员工被解雇、调岗，或不再需要访问数据时，Infor 将立即停用其在包含数据的应用程序或数据存储中的账户。Infor 定期审查有权访问数据的人员及服务清单，并删除不再需要该等访问权限的账户，此类审查至少每半年进行一次。

v. Infor 在任何系统上均不使用制造商提供的默认密码及其他默认安全参数。根据行业公认最佳实践，Infor 强制要求其所有系统使用系统强制执行的“强密码”。Infor 要求所有密码及访问凭证均需保密，不得在人员之间共享；对于已知已被泄露或篡改的密码，Infor 将立即停用。

vi. Infor 设置“账户锁定”机制：当有权访问数据的账户连续输错密码次数超过规定上限时，自动锁定该账户。

vii. 远程访问存储有数据的系统时，需进行双重身份验证（例如，要求至少通过两个独立的身份识别因素验证用户身份）。

1.3 入侵检测与防范

Infor 采用入侵检测系统/入侵防范系统（IDS/IPS），对其系统及相关程序进行监控，排查安全漏洞、违规行为及可疑活动。该监控范围包括可疑外部活动（包括但不限于未授权探测、扫描或入侵尝试）及可疑内部活动（包括但不限于未授权系统管理员访问、未授权系统变更、系统滥用或盗窃、数据处理不当）。Infor 定期审查访问日志，排查恶意行为或未授权访问的迹象。

1.4 防火墙

Infor 已部署并维持网络防火墙技术，旨在保护可通过互联网访问的数据安全。

1.5 更新

Infor 通过升级、更新、漏洞修复及发布新版本等方式，确保系统始终处于最新状态。

1.6 数据加密

i. 数据在公共网络上传输时，至少采用传输层安全协议 1.2 版（TLS 1.2）或其逻辑后续版本进行加密。

ii. 数据在系统中处于静止状态时，至少采用高级加密标准 256 位（AES 256 bit）或其逻辑后续版本进行加密（Infor 转售的 IBM Series i 或 Z 平台解决方案的支持事件除外）。

1.7 身份管理

Infor 采用共享安全模型分配身份管理责任。Infor 可将系统中的应用程序与客户的身份管理提供商进行联合认证，以实现身份验证目的。

1.8 恶意软件

Infor 部署行业公认标准的反恶意软件/反病毒软件，并在可能的情况下启用近实时保护功能，致力于确保所提供的云服务或本地部署软件不含任何“定时炸弹”、“蠕虫”、“病毒”、“特洛伊木马”、“保护代码”、“数据销毁密钥”或其他具有以下意图的编程程序：(i) 针对云服务：篡改、删除、损坏、停用或禁用客户数

据，或阻止、限制客户访问其数据；(ii) 针对本地部署软件：篡改、删除、损坏、停用或禁用本地部署软件中的客户数据。

1.9 物理安全

存放系统的设施应满足以下要求：

- ⅰ. 结构设计能够抵御恶劣天气及其他可合理预见的自然条件；
- ⅱ. 配备适当的物理环境保障措施，防范系统因烟雾、高温、进水、火灾、湿度或电力波动而受损；
- ⅲ. 配备现场备用发电系统；
- ⅳ. 配备适当的控制措施，确保仅授权人员可物理访问该设施。

2. 审计

2.1 审计权利

作为供应商监督计划的一部分，客户及其（如适用）政府监管机构可每年一次通过邮寄审计（即基于 ISO 27001 标准的调查问卷）的形式，要求 Infor 提供与其信息安全计划、流程及控制相关的程序文件。Infor 同意，在该等程序文件可随时获取的情况下，将提供客户合理要求的该等文件，但前提是该等文件不会：(a) 威胁 Infor 其他客户的数据或服务的保密性、完整性或可用性；(b) 违反代表 Infor 向客户提供服务的第三方的数据或服务的保密性、完整性及可用性。Infor 提供的程序文件不包括证明材料（例如但不限于培训证明、测试证明、风险评估结果）。Infor 将在 30 日内回复该调查问卷；若无法在该期限内完成，Infor 将与客户协商确定双方认可的合理完成期限。所有该等文件均属于 Infor 的机密信息。Infor 不认可客户基于该邮寄审计得出的任何结论。

2.2 第三方审计

在订阅期内每 12 个月，Infor 应自费聘请一名合格的独立审计师，对 Infor 与云服务（不含支持服务）相关的既定控制目标及控制活动的设计和运行有效性进行审查。Infor 应促使该审计师为所有云服务编制 SOC I Type 2 报告，并仅为多租户云服务编制 SOC II Type 2 报告（统称“审计报告”）。审计报告属于 Infor 的机密信息，但客户可通过 Infor 支持门户获取。客户可将该审计报告副本分享给其审计师及监管机构，但需告知该等审计师及监管机构：该审计报告属于 Infor 的机密信息，必须予以相应保护。

此外，Infor 应每年自费聘请一名合格的独立审计师，根据国际标准化组织（ISO）27001 标准，对 trust.infor.com 网站上列明的特定多租户云服务，以及本地部署软件和云服务的支持服务相关的信息安全情况进行审查。Infor 应促使该审计师按照该标准编制报告。该审计报告不向客户提供；但客户可随时通过 Infor 云安全网站（trust.infor.com）获取相应的认证证书副本。该证书将明确列明报告所涵盖的软件。作为该 ISO 27001 认证的一部分，Infor 为认证所涵盖的软件及相关支持服务维持一份信息安全管理体系手册，助力确保用于提供该等服务的 Infor 资产的安全性、保密性、完整性及可用性。

更多第三方认证可通过 trust.infor.com 网站查询。

3. 云服务的变更管理

Infor 遵循一套变更控制流程，该流程用于规范 Infor 云服务交付资源内部变更的识别与实施，防范对应用程序源代码、接口、操作系统或现有字段及表格内数据的后端变更造成不必要的影响。所有针对 Infor 云服务交付资源的变更请求，均需遵循实施变更控制流程。Infor 将详细记录其对该流程的遵守情况（例如通过工单系统），并留存所有变更的测试流程记录，包括但不限于变更的日期和时间、变更性质描述。

4. 数据分离；不得利用

4.1 分离

通过适当的技术手段，将数据与 Infor 自身数据及其他任何 Infor 客户的数据进行逻辑分离。

4.2 不得利用；汇总统计数据

数据属于客户的机密信息，客户对其数据拥有全部专有权利。Infor 不得对数据进行商业利用，且仅可在提供服务及履行协议项下义务所需的范围内访问数据。

Infor 通过工具及日志系统收集与客户使用和操作服务相关的统计数据及性能信息（以下简称“汇总统计数据”）。汇总统计数据为 Infor 的专有财产，不被视为数据。

5. 资产管理

Infor 拥有一套正式的资产管理流程，包括维持：

- ⅰ. 用于提供服务的资产清单（以下简称“资产”），旨在识别资产并明确资产的所有权及控制权；
- ⅱ. 用于管理相关资产中数据的归还、销毁或移除的程序；
- ⅲ. 用于保护资产免受内部或外部、故意或意外威胁及漏洞影响的程序。

6. 漏洞扫描与渗透测试

Infor 维持一套漏洞管理流程，用于扫描因利用已公布或已识别的缺陷或弱点（可能被意外或故意利用并导致系统受损或未授权访问）而产生的风险（以下简称“漏洞”）。Infor 将在行业公认的标准期限内处理漏洞，并根据其符合行业公认标准的既定框架，采取与漏洞风险等级相匹配的补救或缓解措施。

Infor 每年自费聘请独立第三方，按照行业公认的标准方法，对多租户云服务进行渗透测试（包括人工手动测试），以评估系统的安全控制效果。

对于多租户订阅软件，在代码发布前及云服务整个产品生命周期内（即开发及生产环境中），将进行安全测试评估（包括源代码扫描及漏洞扫描），以识别需补救或缓解的潜在漏洞。每年将对多租户云服务进行一次渗透测试，以识别需补救或缓解的漏洞。

7. 信息安全事件响应

若 Infor 发现数据已遭受或合理预期可能遭受协议未授权的使用或披露（以下简称“信息安全事件”），Infor 应：(i) 立即且无不当延迟地（无论如何应在知晓该信息安全事件后 48 小时内）通知受影响的客户该事件的发生；(ii) 调查并对该信息安全事件的原因进行合理分析；(iii) 向客户定期更新调查进展；(iv) 制定并实施适当的补救计划，以在 Infor 控制范围内解决该信息安全事件的原因；(v) 配合客户的合理调查，或协助客户遵守与该信息安全事件相关的任何通知或其他监管要求。若发生信息安全事件，经客户请求并由客户承担费用，Infor 应（在法律允许且符合适当保密保护要求的前提下）向客户提供相关系统活动记录的副本（仅限于与客户相关的信息安全事件部分），供客户用于任何法律或监管程序，或任何政府调查。

8. 日志记录与监控

Infor 使用一套专门配置用于管理日志和警报的工具，监控其用于提供服务的资源。日志记录采用物理和虚拟双重安全保护，防范篡改。在任何情况下，均不记录敏感信息及密码。除捕捉服务相关信息外，该监控工具还允许管理员跟踪用户登录和退出系统的活动。

9. 人力资源安全与培训

负责提供服务的 Infor 人员需遵守保密义务，了解信息安全威胁及相关问题，每年至少接受一次常规安全培训，并能够在整体组织信息安全政策框架下，结合自身具体工作职责，落实信息安全政策要求。

10. 终端设备控制（Infor 笔记本电脑、工作站及移动设备）

Infor 采用行业公认的标准安全措施保护终端设备，包括应用程序及操作系统补丁管理自动化，以及反病毒保护。

11. 数据归还与销毁

11.1 归还

云服务终止或到期后，Infor 应在收到客户书面请求（通过提交标准支持工单的方式提出，该请求必须在服务终止后 30 日内提出；单租户客户为 10 日内）后 3-5 个工作日内，通过 Infor 安全文件传输服务，以原生数据库导出格式向客户提供所有客户数据。若客户要求以其他格式归还客户数据，或需要其他终止相关协助服务，Infor 与客户应就该等终止协助服务的范围及应付费用协商一致。在服务终止前，客户可通过应用程序接口访问客户数据；经客户通过支持门户提出请求，Infor 每 12 个月可最多两次通过安全文件传输服务，以原生数据库导出格式向客户提供数据备份副本；超出该次数的请求将产生相应费用。

进一步明确，个人数据的归还和销毁应按照《数据保护协议》的条款执行。

收益系统（例如 Infor 文档管理系统、Infor EzRMS 系统或 Infor 酒店价格优化系统）相关数据将在服务终止时删除，不向客户移交。

11.2 销毁

除客户要求的过渡期协助外，Infor 应在云服务终止或到期后 35 日内，按照美国国家标准与技术研究院（NIST）800-88 标准，永久删除所有（在线或网络可访问的）客户数据实例。

为提供支持服务而向 Infor 提供的数据（即通过登录支持门户提交的支持工单中包含的数据），将在工单关闭之日起 5 年内清除。用于管理支持工单生命周期的客户个人姓名及联系信息（例如用户电子邮件地址、姓名及电话号码），将在支持服务终止时停用并匿名化处理。

12. 分包商

为 Infor 提供与服务相关商品和服务的 Infor 分包商，应按照与本 ISP 实质相似的条款提供该等商品和服务。在聘请任何第三方分包商履行本 ISP 项下任何服务之前，Infor 应尽合理审慎义务对该第三方进行审查，确保其能够遵守本 ISP 项下的保密及安全义务。Infor 对其分包商在支持服务过程中的所有行为承担责任。

免责声明：

以下产品可能适用额外或不同的安全条款：Acumen Invest（Infor 贸易促销管理系统）和 Acumen Radar（Infor 战略定价管理系统）、Anael（SaaS）（法国）；Nexus AppXpress（SaaS）、Nexus Live Visibility（SaaS）、Nexus Factory Management（SaaS）、Nexus Inventory Management（SaaS）、Nexus Supply Chain Finance（SaaS）、Nexus Supply Collaboration（SaaS）、Nexus Transportation

Management（SaaS）、Nexus Supply Chain Visibility（SaaS）、Nexus Procure to Pay（SaaS）、Nexus Supply Chain Intelligence（SaaS）；BPCS/LX、XA、System 21（SaaS）。