信息安全计划

（Information Security Plan）

范畴： 本信息安全计划（“ISP”）已纳入客户与 Infor 签订的协议中（统称“协议”），在本 ISP 条款与协议中的任何其他条款之间发生任何冲突或不一致的情况下，以本 ISP 条款为准。本 ISP 规定了 Infor 当前的安全措施，这些措施旨在保护：

i. Infor 提供的硬件、设备和系统软件配置包括：

a. 云服务（为明确起见，云服务包括支持服务）
b. 专业服务，以及
c. 有关本地部署软件的支持服务

（所有此类硬件、设备和系统软件配置在本 ISP 中统称为“系统”，而云服务、专业服务和本地部署软件支持服务在本 ISP 中统称为“服务”）；同时

ii. 提供给 Infor 的客户数据，可以是：

a. 客户数据，或

b. 为在 Infor 在其环境中实施专业服务和/或支持服务而提供给 Infor 的数据

（所有这些数据在本 ISP 中统称为“数据”）。

定义：本 ISP 中使用的术语如果未在本 ISP 中定义，则其含义应以 Infor 与该客户之间的软件协议（“协议”）中给出的定义为准。

除外内容：本 ISP 不适用以下情况：(i) Infor 在另外的专业服务协议中托管客户的本地部署软件，而根据该协议提供的专业服务，或(ii) 当 Infor 在客户的场所中提供服务和/或在授权访问客户系统。在此类情况下，Infor 应按照工作说明书中双方商定的客户管理、技术和物理情形下进行操作。此外，客户有义务为 Infor 人员提供访问其系统的用户授权和密码，并在其认为适当时撤销授权终止访问。

更新：由于安全威胁以及防范这些安全威胁的措施始终在演变，只要 Infor 从整体上对系统和数据的安全保护维持相同等级或更高等级的水平，Infor 可以随时更新本 ISP 内容且无需通知客户。

1. 一般安全标准

为了防止系统遭到破坏、丢失、或未经授权的访问、更改，Infor 采取了一定的管理、技术和物理保护措施，以确保 Infor 仅在客户的指示下处理客户数据，该系列措施 (i) 不应低于 Infor 对其自有信息中同类信息的保护水平；(ii) 不应低于行业公认的标准；并且 (iii) 应符合相关法律的要求。

1.1 安全官

Infor 已任命一名或多名安全官负责协调和监控本 ISP 中的安全措施。

1.2 访问控制

Infor 对客户数据实施访问控制，包括以下措施：

i. Infor 为每个可访问客户数据的人员分配一个唯一 ID。
ii. Infor 确认有权授予、更改或取消客户数据访问权限的人员，并根据最低权限基础对客户数据的访问权限实施限制。Infor 仅允许为提供服务而“需要知情”的人员访问客户数据，同时留存并更新该等人员记录。该等访问将会记录下来并受到监督。
iii. Infor 要求具有客户数据访问权限的 Infor 人员在计算机无人值守时禁用管理会话功能。
iv. 当 Infor 员工被解聘或调动岗位时，或者当他们不再需要访问客户数据时，Infor 会在包含客户数据的应用或数据存储库中停用他们的账户。Infor 定期审查可访问客户数据的人员名单和服务清单，并删除不再需要该等访问权限的账户。该等审查至少每半年一次。
v. Infor 不会在任何系统上使用制造商提供的默认密码或其他默认安全参数。根据行业公认最佳实践，Infor 所有系统都必须使用系统强制的“强密码”。Infor 要求对所有密码和访问凭证进行保密，不得在员工之间共享，并且 Infor 会停用已知被破坏或泄露的密码。
vi. Infor 还设置了“账户锁定”功能。对于具有客户数据访问权限的账户，如果连续输错密码超过规定次数，则锁定相应账户。
vii. 远程访问存有客户数据的系统需要进行双重身份验证（即需要至少两个独立因素来识别用户身份）。

1.3 入侵检测与预防

Infor 利用入侵检测系统/入侵预防系统 (IDS/IPS) 来监控其系统和程序是否存在安全漏洞、违规行为和可疑活动。这包括了可疑的外部活动（包括但不限于未经授权的探测、扫描或闯入尝试）和可疑的内部活动（包括但不限于未经授权的系统管理员访问、未经授权的系统变更、系统滥用或盗窃或对客户数据的不当处理）。Infor 定期审查访问日志，以寻找恶意行为或未经授权访问的迹象。

1.4 防火墙

Infor 采取网络防火墙技术，以保护可通过互联网访问的客户数据。

1.5 更新

Infor 通过升级、更新、错误修复和发布新版本来确保系统始终处于最新状态。

1.6 数据加密

i. 在公共网络上传输客户数据时，至少要用 TLS 1.2 或其后继版本对数据进行加密。
ii. 当客户数据在系统中处于静止状态时，至少要用 AES 256 位或其后继版本对数据进行加密（但不适用 Infor 转售的 IBM Series i 或 Z 平台解决方案的支持事件）。

1.7 身份管理

Infor 利用共享安全模型来分发安全措施。Infor 可以将系统中的应用与客户身份管理供应商联结起来。

1.8 恶意软件

Infor 安装了行业公认的标准反恶意软件/杀毒软件，并尽可能采用近乎实时的保护措施，以努力确保云服务和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 (i) 针对云服务，企图篡改、删除、损坏、停用或禁用客户数据或阻止或限制客户访问客户数据的程序，或(ii) 针对本地部署软件，企图篡改、删除、损坏、停用或禁用本地部署软件中的客户数据的程序。

1.9 物理安全

系统所处的建筑设施应能够：

i. 在结构上抵御恶劣天气和其他可合理预测的自然条件；
ii. 具有适当的物理环境保护措施来避免系统因烟雾、高温、进水、火灾、湿度或电力波动而受损；
iii. 在现场配有备用发电系统；以及
iv. 具有适当的控制措施，确保仅限授权人员进入设施。

2. 审计

2.1 审计权

作为供应商监督计划的一部分，客户及其政府监管机构（如适用）可以每年一次通过邮寄审计（即基于 ISO 27001 的调查问卷）的形式要求 Infor 提供信息安全计划、流程和控制相关的程序文件。Infor 同意，在该等程序文件可获得的情况下，按照客户的合理要求提供该等文件，前提是该等文件不会 (a) 影响其他 Infor 客户的数据或服务的保密性、完整性或可用性，或 (b) 影响代表 Infor 向客户提供服务的第三方的数据或服务的保密性、完整性和可用性。Infor 提供的程序文件不应包含证明文件（例如培训证明、测试证明、风险评估结果等等）。Infor 会在 30 天内填写调查问卷；如果无法在这一期限内完成，Infor 将与客户共同约定一个完成时间。所有该等文件均属于 Infor 的机密信息。客户基于该等邮寄审计得出的结果不在 Infor 的考虑范围内。

2.2 第三方审计

在订购期内每 12 个月，Infor 会自费聘请一名合格的独立审计师，对 Infor 设定的控制目标以及与云服务（不含支持服务）相关的控制活动的设计和运行效果进行审核。Infor 将促使该审计师为所有云服务准备 SOC I 类型 2 报告，为多租户云服务准备的仅为 SOC II 类型 2 报告（统称为“审计报告”）。计报告属于 Infor 的机密信息，但客户可通过 Infor 支持门户网站获得此报告。客户可以向其审计师和监管机构分享该等审计报告的副本，前提是告知审计师和监管机构该等审计报告属于 Infor 的机密信息，必须受到相应保护。

此外，在订购期内每 12 个月，Infor 应自费聘请一名合格的独立审计师，根据国际标准化组织 ISO27001 的要求对 trust.infor.com 上的某些多租户云服务以及本地部署软件和云服务中的支持服务进行信息安全审查。Infor 应要求该审计师按照该标准编制报告。审计报告不会提供给客户；但客户可随时

通过 Infor 的云安全网站 (trust.infor.com) 获取结果证书的副本。证书中会标识受报告约束的软件。同时，作为 ISO 27001 证书的一部分，对于证书中包含的软件及相关支持服务，Infor 还会保存一份信息安全管理系统手册，以确保提供该服务的 Infor 资产的安全性、保密性、完整性和可用性。

在 trust.infor.com 网站上可以获取更多第三方证书信息。

3. 云服务的变更管理

Infor 遵循变更控制流程，该流程旨在对 Infor 提供的云服务所做变更的识别与实施进行管理，从而防止对应用源代码、界面、操作系统进行不必要的变更，或对现有字段和表格内的数据进行后端变更。为遵循该变更控制流程，Infor 保留详细记录，例如问题录入系统，以及对变更信息的任何测试记录其中包括了变更的时间日期及变更性质的描述等等。

4. 客户数据分离；无开发

4.1 分离

Infor 将通过恰当的技术手段将客户数据与 Infor 数据及其他 Infor 客户的数据分开。

4.2 无开发；汇总的统计信息

客户数据属于客户机密信息，客户拥有对其数据的所有专属权利。Infor 不会对客户数据进行商业开发，除了提供服务和履行协议义务所需之外，不会访问客户数据。

Infor 可能会收集汇总的统计信息，这些信息属于 Infor 的专有财产而不视作为客户数据。“汇总的统计信息”是通过仪器和日志系统生成的与客户使用、操作服务相关的统计数据和性能信息。

5. 资产管理

Infor 有资产管理流程，包括:

i. 维护用于提供服务的资产清单（“资产”），建立明确的资产所有权和控制权，开发识别资产的功能，
ii. 管理相关资产中客户数据的归还、销毁或移除的程序；以及
iii. 用于保护资产免受内部或外部、故意或意外威胁和漏洞的程序。

6. 漏洞扫描和渗透测试

Infor 有漏洞管理流程，用于扫描利用已公布或已确定的缺陷或弱点而产生的风险，这些缺陷或弱点能够被（意外或故意地）利用，并导致系统受损或可能发生未经授权访问系统（“漏洞”）。Infor 会在行业公认的标准期限内解决漏洞问题。Infor 应根据其符合行业公认标准的框架，以合适的方式弥补或减少漏洞。

每年，Infor 都自费聘请独立的第三方按照行业公认的方法开展包含人工测试的渗透测试，以评估多租户系统的安全控制情况。

对于多租户订购软件，在代码发布前以及云服务的整个生命周期内（即在开发和生产环境中）进行安全测试评估，包括源代码扫描和漏洞扫描，以识别需要补救或缓解的潜在漏洞。多租户系统的渗透测试每年都会开展，以确定需要补救或减少的漏洞。

7. 信息安全事件响应措施

如果 Infor 意识到客户数据已经或经合理预期可能受到未经本 ISP 授权的使用或披露（“信息安全事件”），Infor 应： (i) 立即通知客户发生了信息安全事件（知晓安全事件的 48 小时内）；(ii) 调查并分析此类信息安全事件的原因；(iii) 对调查进展定期向客户定期更新；(iv) 制定并实施适当的计划，以便在 Infor 控制范围内对信息安全事件的原因进行补救；以及 (v) 配合客户合理范围内开展调查活动、协助客户应对监管机构对此类信息安全事件发出的征询或提出的其他要求。发生信息安全事件时，经客户要求、且费用由客户承担的情况下，Infor 可以（在法律允许的范围内并在采取适当保密措施的前提下）向客户提供相关系统活动记录的副本（仅限于与特定客户相关的信息安全事件），用于法律、监管程序或客户接受的政府调查。

8. 记录和监控

Infor 运用经专门配置用于管理日志和报警的工具来监控其提供服务的资源。日志记录均以物理方式和虚拟方式安全保存，以防篡改。在任何情况下都不会记录敏感信息和密码。除了捕捉服务相关信息外，管理员还可使用监控工具来追踪用户进入和退出系统的操作。

9. 人力资源安全性及培训

提供服务的 Infor 人员必须遵守保密义务，掌握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，并且能够在一般情况下以及在其具体工作职能范围内支持信息安全政策的实施。

10. 终端设备控制（Infor 笔记本电脑、工作站和移动设备）

Infor 采取行业公认的安全措施实施终端保护，包括应用程序和操作系统补丁管理自动化及防病毒保护。

11. 数据归还与销毁

11.1 归还

云服务终止或到期后，Infor 应及时（在收到客户的书面请求后 3-5 个工作日内）通过 Infor FTP 服务器将客户数据导出本地数据库归还给客户。如果客户要求以其他替代格式归还客户数据或要求其他协助服务，Infor 和客户双方应就此类协助服务的范围和费用进行协商。在服务终止之前，客户可以通过应用程序接口访问客户数据，当客户通过支持门户提出请求后， Infor可以提供每12个月最多两次的数据备份副本，以原生数据库导出的形式通过Infor的安全文件传输服务提供；超出的请求需支付费用。

需进一步明确的是，个人数据的归还和销毁依据《数据保护协议》执行。

11.2 销毁

除了客户要求的过渡期协助外，Infor将在云服务终止或到期后的35天内，根据NIST 800-88的标准，永久删除所有（在线或网络可访问的）客户数据。

基于支持服务而提供给Infor的数据（即通过登录到支持门户的支持工单）将在工单关闭日期后的5年内清除。用于管理支持工单生命周期的客户个人姓名和联系信息（例如，用户电子邮件地址、姓名和电话号码）将在支持服务终止时停用并同时匿名化。

12. 分包商

Infor 的分包商在提供与 Infor 服务相关的商品和服务时，应按照与本ISP相似的条款操作。在聘请第三方分包商履行任何服务之前，Infor 应尽合理义务对分包商进行审查，以确保该第三方能够遵守保密和安全义务。Infor 应对支持其服务的分包商的所有行为负责。

免责声明：以下产品可能适用不同的安全条款：Acumen Invest (Infor Trade Promotions Management) and Acumen Radar (Infor Strategic Pricing Management), 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）。