Nexus* Information Security Plan

**Applicable Nexus Products: 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)*

This Information Security Plan ("ISP") is incorporated into the Order Form between Infor and the Customer named therein and sets forth Infor's current security measures that are designed to safeguard the hardware, equipment, and systems software configuration (i) on which Infor supports use of the Subscription Software (set forth in the Order Form) and the related Subscription Services and (ii) in which Customer Data has been provided, entered or uploaded for use by or with the Subscription Software by Customer or its Authorized Users (i and ii collectively, the "Systems"). For clarity, capitalized terms used in this ISP and not defined within this ISP have the meaning given such terms in the Software as a Service Agreement between Infor and such Customer (the "Agreement"). This ISP is not applicable to Infor managed service arrangements, where Customer's on-premise software is hosted by Infor pursuant to a separately negotiated professional services agreement.

Security threats, and the measures designed to protect against those security threats, are continually evolving, and Infor may change this ISP at any time without notice to Customer, provided Infor maintains a comparable or better level of security in the aggregate for the Systems and Customer Data.

1. General Security Standards

Infor maintains administrative, technical, and physical safeguards designed to protect against the destruction, loss, unauthorized access or alteration of the Systems, and the Customer Data Infor processes at the direction of the Customer, which are: (i) no less rigorous than those maintained by Infor for its own information of a similar nature; (ii) no less rigorous than generally accepted industry standards; and (iii) required by applicable laws.

1.1. Security Officers

Infor has appointed one or more security officers responsible for coordinating and monitoring the security measures in this ISP.

1.2. Access Controls

Infor implements access controls to Customer Data, including the following measures:

i. Infor assigns a unique ID to each person with computer access to Customer Data.

ii. Infor identifies personnel who may grant, alter or cancel access to Customer Data, and restricts access to Customer Data on a least-privilege basis. Access to Customer Data is allowed only to personnel who have a "need-to-know" for delivering Subscription Services, and Infor maintains and updates a record of such personnel. Such access is logged and monitored.

iii. Infor instructs Infor personnel having access to Customer Data to disable administrative sessions when computers are left unattended. Applications use session timeouts to disable sessions after a specified period of time.

iv. Infor deactivates Infor's employees' accounts from applications or data stores which contain Customer Data when such employees are terminated or transferred, or when they no longer require access to such Customer Data. Infor regularly reviews the list of people and services with access to Customer Data and removes accounts that no longer require such access. Infor performs this review biannually at a minimum.

v. Infor does not use manufacturer-supplied defaults for passwords and other security parameters on any Systems. Infor mandates the use of system-enforced "strong passwords," according to generally accepted industry best practices on all Infor's Systems. Infor requires that all passwords and access credentials be kept confidential and not be shared among personnel, and Infor deactivates passwords that are known to have been corrupted or disclosed.

v. Infor maintains an "account lockout" by disabling accounts with access to Customer Data when an account exceeds a specified number of incorrect password attempts.

vi. Remote access to Systems holding Customer Data requires two-factor authentication (e.g., requires at least two separate factors for identifying users).

1.3. Intrusion detection and Prevention

Infor utilizes an intrusion detection system/intrusion prevention system (IDS/IPS) to monitor its Systems and its procedures for security breaches, violations and suspicious activity. This includes suspicious external activity (including, without limitation, unauthorized probes, scans or break-in attempts) and suspicious internal activity (including, without limitation, unauthorized system administrator access, unauthorized changes to the Systems, Systems misuse or theft, or mishandling of Customer Data). Infor regularly reviews access logs for signs of malicious behavior or unauthorized access.

1.4. Firewall

Infor has implemented and maintains network firewall technologies designed to protect Customer Data accessible from the Internet.

1.5. Updates

Infor keeps the Systems up-to-date with upgrades, updates, bug fixes, and new versions.

1.6. Data Encryption

i. In transit over public networks, Customer Data is encrypted with, at a minimum, TLS 1.2 or its logical successor.

ii. While Customer Data is at rest within Systems, Customer Data is encrypted with, at a minimum, AES 256 bit or its logical successor.

1.7. Identity Management

Infor leverages a shared security model to distribute responsibility for identity management. Infor has the ability to federate the applications in the Systems back to Customer's identity management provider for authentication purposes.

1.8. Single Sign On

Infor Nexus support Single Sign On [SSO] central system at Customer's organization to act as an "Identity Provider" (IDP) to log into Infor Nexus. Infor Nexus supports any identification system using SAML2 standard, as a standard SSO central IDP requires. Customer Single Sign On is assumed to have two factor authentication.

1.9. Security Guidelines

Infor Nexus authentication recommendations are prepared in accordance with guidelines from the US National Institute of Standards and Technology (NIST) and generally accepted industry best practices.

1.10. Two Factor Security System

Infor Nexus always recommends the use of two factor authentication. User can use the Infor Nexus mobile app for the 2nd factor for authentication. However, users of the Procure to Pay product are required to use two factor authentication.

1.11. Password Management

In cases where Single Sign on is not available, Infor Nexus Customers will configure their password policy on top of the minimum defaults of the system. All accounts for the Customer will adhere to that password policy.

The default password settings are:

- All passwords are checked against a list of the most common passwords based on data breaches. Passwords which appear on this list are not allowed
- All passwords must be at least 8 characters long
- Spaces are allowed in passwords, and the use of an easy-to-remember phrase is encouraged
- None of the following are allowed, unless there are at least 8 (or the configured minimum, greater than 8) additional characters in the password:
    - User's first or last name
    - User's login
    - Any word in user's organization name greater than three characters
    - User or organization's phone number and fax number
    - User's email address

1.12. Built in Measures

To prevent brute force password breaking, a throttling algorithm will prevent password guesses. Customers can configure their passwords policy

- Minimum password length (greater than 8)

- Enforced use of both uppercase and lowercase letters in the password
- Enforced use of numerals in the password
- Enforced use of symbols in the password
- Enforced use of *either* numeral or symbol in the password
- Password expiry after a certain number of days
- User accounts locked after a certain number of password attempts

The minimum password is 8 by default and cannot be set *lower*. The rest of these settings, in accordance with modern best practices, are *not* set by default, but can be configured for Customer organizations by Infor Nexus as part of implementation.

1.13. Malicious Software

Infor maintains generally accepted industry standard anti-malware/anti-virus software and, to the extent possible, uses near real-time protection features in an effort to provide Subscription Software and Subscription Services that do not contain any "time bombs," "worms," "viruses," "Trojan horses," "protect codes," "data destruct keys," or other programming devices that are intended to access, modify, delete, damage, deactivate or disable Customer Data or to prevent or limit Customer's access to Customer Data ("Malicious Code").

1.14. Physical Security

Facilities containing the Systems will:

i. be structurally designed to withstand adverse weather and other reasonably predictable natural conditions;

ii. have appropriate physical environmental safeguards to help protect Systems from damage related to smoke, heat, water, fire, humidity, or fluctuations in electrical power;

iii. be supported by on-site backup power generating systems; and

iv. have appropriate controls designed to ensure that only authorised personnel are allowed physical access to the facility.

2. Audit

2.1. Audit Rights

As part of its vendor oversight program, Customer and (if applicable) its governmental regulatory agency may request, once per year in the form of a postal audit (i.e. a questionnaire that is based on ISO 27001), procedural documentation from Infor regarding its information security program, processes and controls. Infor agrees that to the extent such procedural documentation is readily available, Infor will supply such documentation that Customer may reasonably request, so long as such documentation does not (a) threaten the confidentiality, integrity or availability of data or services of Infor's other customers or (b) violate the confidentiality, integrity and availability of data or services of third parties providing Subscription Services to customer on behalf of Infor. Procedural documentation provided by Infor will not include evidence (for example, but not limited to, proof of training, proof of testing, results of risk assessments). Infor will respond to the questionnaire within 30 days; if this timeframe cannot be met, Infor will work with the Customer to arrive at an agreement

for completion. All such documentation shall be Infor's Confidential Information. Infor will not consider Customer findings resulting from this postal audit.

2.2. Third Party Audit

Once in each 12-month period during the Subscription Term, Infor shall, at its cost and expense, engage a duly qualified independent auditor to conduct a review of the design and operating effectiveness of Infor's defined control objectives and control activities in connection with the Subscription Services. Infor shall cause such auditor to prepare a report in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18) or an equivalent standard, which may include ISAE 3402 (the "Audit Report"). The Audit Report is Infor's Confidential Information, but is available to Customer on the Infor support portal. Customer may share a copy of such Audit Report with its auditors and regulators, provided that the auditors and regulators are informed that such Audit Report is Infor's Confidential Information and must be protected accordingly.

3. Change Management

Infor follows a change control process that governs the identification and implementation of changes within Infor's Subscription Services delivery resources to help prevent unwanted changes to application source code, interfaces, operating systems or back-end changes to data within existing fields and tables. All requested changes to Infor's Subscription Services delivery resources must follow an implementation change control process. Infor documents and retains a detailed record of its compliance with this process, such as a ticketing system, and records of testing procedures for any change, including without limitation the date and time of any such change and a description of the nature of the change.

4. Segregation of Customer Data; No Exploitation

4.1. Segregation

Customer Data is kept logically separated from Infor's data and the data of any other Infor customer by appropriate technical means.

4.2. No Exploitation; Aggregated Statistics

Customer Data is the Confidential Information of Customer, and Customer owns all proprietary rights to its Customer Data. Infor will not commercially exploit Customer Data and will not access Customer Data other than as needed to perform Subscription Services and fulfil its obligations in accordance with the Agreement.

Infor may collect Aggregated Statistics, which are the sole property of Infor and are not considered Customer Data. "Aggregated Statistics" are statistical data and performance information, generated through instrumentation and logging systems, regarding Customer's use and operation of the Subscription Software and Subscription Services.

5. Asset Management

Infor has a formal asset management process that includes:

i. maintaining an inventory of assets used to provide Subscription Services ("Assets"), establishing clear ownership and control of Assets, being capable of identifying Assets, and managing the return, destruction, or removal of Customer Data from applicable Assets; and

ii. procedures designed to protect Assets from threats and vulnerabilities, whether internal or external, deliberate or accidental.

6. Vulnerability Scanning and Penetration Testing

Infor maintains a vulnerability management process to scan for risks resulting from exploitation of published or identified flaws or weaknesses that could be exercised (accidentally or intentionally) and result in harm or unauthorized access to the Systems ("Vulnerabilities"). Infor will address Vulnerabilities within generally accepted industry standard time frames. Infor shall remediate or mitigate Vulnerabilities in a manner commensurate with the risk those Vulnerabilities represent, according to Infor's defined framework, which is consistent with generally accepted industry standards.

On an annual basis, Infor engages, at its own cost, an independent third party to conduct penetration testing, including human manual testing, to evaluate the security controls of multi-tenant Systems following generally accepted industry standard methodologies.

For multi-tenant Subscription Software, security testing assessments, including source code scans and Vulnerability scans, are conducted prior to code release and throughout the Subscription Software product lifecycle (i.e., in development and production environments) to help identify potential Vulnerabilities for remediation or mitigation. On an annual basis penetration testing is performed on multi-tenant Systems to identify Vulnerabilities for remediation or mitigation.

7. Information Security Incident Response

If Infor becomes aware that Customer Data has been, or is reasonably expected to be, subject to a use or disclosure not authorized by this ISP (an "Information Security Incident"), Infor shall: (i) promptly and without undue delay (and in any event within 48 hours of becoming aware of such Information Security Incident), notify Customer of the occurrence of such Information Security Incident; (ii) investigate and conduct a reasonable analysis of the cause(s) of such Information Security Incident; (iii) provide periodic updates of any ongoing investigation to Customer; (iv) develop and implement an appropriate plan to remediate the cause of such Information Security Incident to the extent such cause is within Infor's control; and (v) cooperate with Customer's reasonable investigation or Customer's efforts to comply with any notification or other regulatory requirements applicable to such Information Security Incident. Upon Customer's request, and at Customer's expense, in the event of an Information Security Incident, Infor shall deliver (to the extent allowed by law and subject to appropriate confidentiality protections) copies of records of applicable Systems activity (solely with respect to the Information Security Incident as it relates to Customer) to Customer for use in any Customer legal or regulatory proceeding or in any Customer governmental investigation.

8. Logging and Monitoring

Infor monitors its resources used to provide Subscription Services using a set of tools, specifically configured to manage logs and alerts. Log records are kept physically and virtually secured to help prevent tampering. Sensitive information and passwords are not logged under any circumstances. In addition to capturing service-related information, the monitoring tools allows administrators to keep track of user activity when entering and exiting the system.

9. Human Resource Security

Infor personnel delivering Subscription Services are subject to confidentiality obligations, are knowledgeable regarding information security threats and concerns, receive general security training

at least annually, and are equipped to support organizational information security policies in general as well as within their specific job functions.

10. Endpoint Device Controls (Infor Laptop, Workstations, and Mobile Devices)

Infor implements generally accepted industry practice security measures for the protection of endpoints including application and operating system patch management automation and anti-virus protection.

11. Data Return and Destruction

11.1. Return

Customer has access to its data throughout the term of its subscription, subject to scheduled downtime, emergency maintenance and other service level availability guidelines. If Customer requires the return of Customer Data in a nonstandard format or requires any other termination assistance services, Infor and Customer shall mutually agree upon the scope of such termination assistance services and the fees and expenses payable for such termination assistance services. Notwithstanding the foregoing, Shared Data must remain on the Infor Nexus Platform as it is not owned by Customer, it is shared. Shared Data is any data that is visible to both Customer/Member and one or more additional authorized members on the Infor Nexus Platform, such as suppliers and service providers. Data is stored at the transaction level and and not customer level.

11.2. Destruction

Infor will use generally accepted industry-standard processes to dispose of hardware and physical components containing Customer Data. All storage is electronically wiped (zeroed) prior to being deployed or decommissioned from the Infor production environment.

12. Subcontractors

Infor subcontractors furnishing goods and services to Infor with respect to Infor's Subscription Services shall furnish such goods and services on terms substantially similar to those set forth in this ISP. Before engaging such third party subcontractor to perform any of the Subscription Services hereunder, Infor shall vet such third party with reasonable diligence in order to help ensure that such third party can comply with the confidentiality and security obligations hereunder. Infor is responsible for all actions of its subcontractors in supporting the Subscription Services.