Information Security Plan

Scope: This Information Security Plan ("ISP") is incorporated into Customer's agreements executed with Infor (collectively, the "***Agreements***"). In the event of any conflict or inconsistency between the terms of this ISP and any other terms in the Agreements, this ISP shall prevail. This ISP sets forth Infor's current security measures that are designed to safeguard, with respect to all Customers generally:

i. the hardware, equipment, and systems software configuration on which Infor provides:

   a. Cloud Services (for clarity Cloud Services includes Support)
   b. Professional Services, and
   c. Support with respect to On-Premises Software

   (all such hardware, equipment, and systems software configuration are collectively defined in this ISP as the "Systems", and the Cloud Services, Professional Services and On-Premises Software Support are collectively defined in this ISP as the "Services"); as well as

ii. Customer data provided to Infor, either:

   a. as Customer Data, or
   b. as provided to Infor for purposes of performing Professional Services and/or Support from within Infor's environment

   (all such data is collectively defined in this ISP as "Data").

Definitions: Capitalized terms used in this ISP and not defined within this ISP have the meaning given such terms in the Software Agreement between Infor and such Customer (the "Agreement").

Exclusions: This ISP is not applicable: (i) to Infor Professional Services arrangements where Customer's On-Premises Software is hosted by Infor pursuant to a separately negotiated Professional Services agreement, or (ii) when Infor is performing services on the Customer's premises and/or is given access to Customer's systems. In such cases, Infor shall comply with Customer's administrative, technical, and physical conditions as mutually agreed in a statement of work, and in connection with any such access to Customer's systems Customer shall be responsible for providing Infor personnel with user authorizations and passwords to access its systems and revoking such authorizations and terminating such access, as Customer deems appropriate.

Updates: 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 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 Data 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. Infor has no responsibility for products and services that interoperate with the Systems and Customer (a) develops,

© 2026 Infor (US), LLC

or has developed, for itself (outside of development through Infor tooling/APIs), or (b) licenses under such third parties' own applicable license terms.

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 Data, including, without limitation, the following measures:

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

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

iii. Infor instructs Infor personnel with access to Data to disable administrative sessions when computers are left unattended.

iv. Infor deactivates Infor's employees' accounts from applications or data stores which contain Data when such employees are terminated or transferred, or when they no longer require access to such Data. Infor regularly reviews the list of people and services with access to 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.

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

vii. Remote access to Systems holding 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 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 Data accessible from the Internet.

© 2026 Infor (US), LLC

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, Data is encrypted with, at a minimum, TLS 1.2 or its logical successor.

ii. While Data is at rest within Systems, Data is encrypted with, at a minimum, AES 256 bit or its logical successor (other than with respect to Support incidents for Infor resold IBM Series i or Z platform solutions).

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. 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 Cloud Services, or On-Premises Software, that do not contain any "time bombs", "worms", "viruses", "Trojan horses", "protect codes", "data destruct keys", or other programming devices that are intended to (i) with respect to Cloud Services, modify, delete, damage, deactivate or disable Customer Data or to prevent or limit Customer's access to Customer Data or (ii) with respect to On-Premises Software, modify, delete, damage, deactivate or disable Customer's data within the On-Premises Software.

1.9. 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

© 2026 Infor (US), LLC

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 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 a mutually agreed to reasonable time frame 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 Cloud Services (excluding Support). Infor shall cause such auditor to prepare a SOC I Type 2 report for all Cloud Services and, for multi -tenant Cloud Servicesonly, a SOC II Type 2 report (collectively, 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.

In addition, Infor shall annually, at its cost and expense, engage a duly qualified independent auditor to conduct a review of its information security in connection with certain multi-tenant Cloud Services stated on trust.infor.com, as well as Support for both On Premises Software and Cloud Services, in each case under the International Organization for Standardization (ISO) 27001 standard. Infor shall cause such auditor to prepare a report in accordance with such standard. The audit report will not be available to Customer; however Customer may obtain a copy of the resulting certificate from Infor's cloud security site (trust.infor.com) at any time. The certificate will identify the software subject to the report. As part of this ISO 27001 certification, Infor maintains an Information Security Management System manual for the software included in the certification, and the related Support, which helps to ensure the protection, confidentiality, integrity and availability of Infor assets used to provide such Services.

Additional third party certifications are available at trust.infor.com.

3. Change Management for Cloud Services

Infor follows a change control process that governs the identification and implementation of changes within Infor's Cloud 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 Cloud 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 Data; No Exploitation

4.1. Segregation

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

© 2026 Infor (US), LLC

4.2. No Exploitation; Aggregated Statistics

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

Infor collects statistical data and performance information, generated through instrumentation and logging systems, regarding Customer's use and operation of the Services ("Aggregated Statistics"). Aggregated Statistics are the sole property of Infor and are not considered Data.

5. Asset Management

Infor has a formal asset management process that includes maintaining:

i. an inventory of assets used to provide Services ("Assets") designed to identify and establish clear ownership and control of Assets;

ii. procedures designed to manage the return, destruction, or removal of Data from applicable Assets; and

iii. 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 for multi-tenant Cloud Services, including human manual testing, to evaluate the security controls of 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 Cloud Services 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 Cloud Services to identify Vulnerabilities for remediation or mitigation.

7. Information Security Incident Response

If Infor becomes aware that Data has been, or is reasonably expected to have been, subject to a use or disclosure not authorized by the Agreement (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 an affected 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

© 2026 Infor (US), LLC

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 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 and Training

Infor personnel delivering 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

Upon termination or expiration of Cloud Services, Infor shall promptly (within 3-5 business days upon receipt of Customer's written request by submission of a standard Support ticket, which request must be made within 30 days of termination (10 days for single-tenant)) make all Customer Data available to Customer as a native database export provided through Infor's secure file transfer service. If Customer requires the return of Customer Data in an alternate 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. Prior to termination, Customer has access to Customer Data through application interfaces, and Infor shall return, upon Customer request made through the Support portal, copies of data backups up to two times per 12 month period as a native database export provided through Infor's secure file transfer service; additional requests will be subject to fees.

Further for clarity, the return or destruction of Personal Data will be in accordance with the terms of the Data Protection Agreement.

Data for yield systems (e.g. Infor Document Management, Infor EzRMS or Infor Hospitality Price Optimizer) are deleted on termination and not transferred to Customer.

11.2. Destruction

© 2026 Infor (US), LLC

Other than with respect to Customer requested Transition Assistance, Infor will permanently delete all (online or network accessible) instances of Customer Data within 35 days after the termination or expiration of Cloud Services in accordance with NIST 800-88.

Data provided to Infor for purposes of performing Support (i.e. through a Support ticket logged into the Support portal) is purged five years from incident ticket closure date. Customer individual name and contact information (e.g. user email address, name, and phone number) used to manage Support ticket lifecycle is deactivated and anonymized on termination of Support.

12. Subcontractors

Infor subcontractors furnishing goods and services to Infor with respect to Infor's 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 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 Services.

*Disclaimer: The following products may have additional or different security terms: Acumen Invest (Infor Trade Promotions Management) and Acumen Radar (Infor Strategic Pricing Management)**,** Anael (SaaS) (France); 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).*

© 2026 Infor (US), LLC