Piano per la Sicurezza delle Informazioni di Nexus*

REVISIONI IN VIGORE NOVEMBRE 2023

**Prodotti Nexus applicabili: 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)*

Oggetto: Il presente Piano per la Sicurezza delle Informazioni (Information Security Plan, "ISP") è incorporato negli accordi che il Cliente conclude con Infor (collettivamente, gli "**Accordi**"). In caso di conflitto o incoerenza tra i termini del presente ISP e ogni altro termine degli Accordi, prevarranno le previsioni del presente ISP. Il presente ISP stabilisce le attuali misure di sicurezza di Infor, le quali sono progettate per salvaguardare:

(i) l'hardware, le attrezzature e la configurazione software dei sistemi di cui Infor si avvale per fornire Servizi Cloud (per chiarezza, i Servizi Cloud includono il Supporto) e Servizi Professionali (tutte le configurazioni software di hardware, apparecchiature e sistemi sono definite collettivamente in questo ISP come i "Sistemi" e i Servizi Cloud e i Servizi Professionali sono definiti collettivamente in questo ISP come i "Servizi") così come

(ii) i dati del Cliente forniti a Infor:
- come Dati del Cliente o,
- come forniti a Infor allo scopo di eseguire Servizi Professionali e/o Supporto dall'interno dell'ambiente di Infor

(tutti questi dati sono definiti collettivamente in questo ISP come "Dati")

Definizioni: i termini in maiuscolo utilizzati nel presente ISP e non definiti all'interno dello stesso hanno il significato attribuito loro nel Contratto Software per Servizi Cloud stipulato tra Infor ed il Cliente in questione (il "Contratto").

Esclusioni: Il presente ISP non è applicabile nel caso in cui Infor esegua i servizi presso i locali del Cliente e/o abbia accesso ai sistemi del Cliente. In tali casi, Infor rispetterà le condizioni amministrative, tecniche e fisiche del Cliente concordate in uno *statement of work*. In relazione a tale accesso ai sistemi del Cliente, il Cliente dovrà fornire al personale di Infor le autorizzazioni utente e le password necessarie per accedere ai propri sistemi e di revocare tali autorizzazioni e accessi, non appena il Cliente lo ritenga opportuno.

Aggiornamenti: Le minacce alla sicurezza e le misure progettate per proteggersi da tali minacce sono in continua evoluzione e Infor potrà modificare il presente ISP in qualsiasi momento senza darne preventiva comunicazione al Cliente, a condizione che Infor adotti un livello di sicurezza equivalente o migliore nel complesso per i Sistemi e i Dati.

1. Standard Generali di Sicurezza

Infor adotta misure di sicurezza amministrative, tecniche e fisiche progettate per proteggere contro la distruzione, la perdita, l'accesso non autorizzato o l'alterazione dei Sistemi e dei Dati . Dette misure di sicurezza sono: (i) non meno rigorose di quelle adottate da Infor per le proprie informazioni di natura analoga; (ii) non meno rigorose degli standard di settore generalmente accettati; e (iii) richieste dalle leggi applicabili.

1.1. Responsabili della Sicurezza

Infor ha nominato uno o più responsabili della sicurezza incaricati di coordinare e monitorare le misure di sicurezza del presente ISP.

1.2. Controlli di Accesso

Infor implementa controlli sull'accesso ai Dati, che includono, a titolo esemplificativo ma non esaustivo, le seguenti misure:

i. Infor assegna un ID univoco a ciascuna persona che ha accesso informatico ai Dati.

ii. Infor identifica il personale che può concedere, modificare o revocare l'accesso ai Dati e limita l'accesso ai Dati in base al principio del c.d. "privilegio minimo". L'accesso ai Dati è consentito solo al personale che ha la "necessità di conoscere" tali Dati per la prestazione dei Servizi e Infor conserva e aggiorna un registro di tale personale. L'accesso ai Dati è registrato e monitorato.

iii. Infor istruisce il proprio personale che ha accesso ai Dati affinché disabiliti le sessioni amministrative quando i computer sono lasciati incustoditi. Le applicazioni utilizzano i timeout delle sessioni per disabilitare le sessioni dopo un periodo di tempo specificato.

iv. Infor disattiva gli account dei propri dipendenti dalle applicazioni o dagli archivi di dati che contengono i Dati quando tali dipendenti vengono licenziati o trasferiti oppure quando non hanno più la necessità di accedere a tali Dati. Infor rivede regolarmente l'elenco delle persone e dei servizi che hanno accesso ai Dati e rimuove gli account che non hanno più necessità di accedervi. Infor esegue questa revisione almeno ogni due anni.

v. Infor non utilizza valori predefiniti forniti dal produttore per le password e per altri parametri di sicurezza su nessun Sistema. Infor impone, su tutti i Sistemi Infor, l'uso di "password forti" richieste dal sistema, secondo le migliori prassi di settore generalmente accettate. Infor richiede che tutte le password e le credenziali di accesso siano mantenute riservate e non vengano condivise tra il personale. Infor disattiva le password che risultano essere state corrotte o divulgate.

vi. Infor effettua un "blocco degli account" disabilitando gli account con accesso ai Dati quando un account supera più un determinato numero di tentativi di inserimento di una password errata.

vii. L'accesso da remoto ai Sistemi che contengono i Dati richiede un'autenticazione a due fattori (ad esempio, richiede almeno due distinti fattori per identificare gli utenti).

1.3. Rilevamento e Prevenzione delle Intrusioni

Infor utilizza un sistema di rilevamento delle intrusioni/sistema di prevenzione delle intrusioni (IDS/IPS) per monitorare i propri Sistemi e le proprie procedure per violazioni della sicurezza, infrazioni e attività sospette. Ciò include attività esterne sospette (tra cui, a mero titolo esemplificativo, sonde non autorizzate, scansioni o tentativi di intrusione) e attività interne sospette (tra cui, a mero titolo esemplificativo, l'accesso non autorizzato dell'amministratore di sistema, le modifiche non autorizzate ai Sistemi, l'uso improprio o il furto dei Sistemi, o la gestione non corretta dei Dati). Infor esamina regolarmente i registri degli accessi alla ricerca di segnali di comportamenti dannosi o di accessi non autorizzati.

1.4. Firewall

Infor ha implementato e mantiene una tecnologia firewall di rete progettata per proteggere i Dati accessibili da Internet.

1.5. Aggiornamenti

Infor mantiene i Sistemi aggiornati con upgrade, aggiornamenti, correzioni di bug e nuove versioni.

1.6. Crittografia dei Dati

i. Nel transito su reti pubbliche, i Dati sono criptati, almeno, con TLS 1.2 o il suo successore logico.

ii. Quando i Dati sono inattivi all'interno dei Sistemi, i Dati sono criptati, almeno, con AES 256 bit o il suo successore logico.

1.7. Gestione dell'Identità

Infor utilizza un modello di sicurezza condiviso per gestire la sicurezza. Infor è in grado di associare le applicazioni dei Sistemi al fornitore dei servizi di gestione delle identità del Cliente.

1.8. Single Sign On

Infor Nexus supporta un sistema centrale di Single Sign On [SSO] utilizzando i sistemi di terze parti di un Cliente come identity provider (IDP) e Infor Nexus come fornitore di servizi. Infor Nexus supporta qualsiasi sistema di provider di identità che utilizza gli standard SAML (Security Assertion Markup Language) 2.0. Si presume che il Single Sign On del Cliente abbia un'autenticazione a due fattori.

1.9. Linee Guida per la Sicurezza

Le raccomandazioni per l'autenticazione di Infor Nexus sono state elaborate in conformità alle linee guida del National Institute of Standards and Technology (NIST) statunitense e alle migliori pratiche di settore generalmente accettate.

1.10. Sistema di Sicurezza a Due Fattori

Infor Nexus raccomanda sempre l'uso dell'autenticazione a due fattori. Gli utenti possono utilizzare l'applicazione mobile Infor Nexus come secondo fattore di autenticazione. In ogni caso, gli utenti del prodotto Procure to Pay sono tenuti a utilizzare l'autenticazione a due fattori.

1.11. Gestione delle Password

Nei casi in cui il Single Sign On non sia disponibile, i Clienti di Infor Nexus sono responsabili della configurazione di una policy per le password che soddisfi gli standard di sicurezza aziendali. Tutti gli account del Cliente dovranno rispettare tale policy sulla gestione delle password.

Di seguito le impostazioni predefinite per le password:

- tutte le password vengono verificate rispetto a password realmente utilizzate e , precedentemente esposte in caso di *data breach*. Le password presenti in questo elenco non sono consentite;
- tutte le password devono essere composte da almeno 8 caratteri;
- sono consentiti gli spazi nelle password e si incoraggia l'uso di una frase facile da ricordare;
- non è consentito l'uso delle seguenti espressioni, a meno che non vi siano almeno 8 (o il numero minimo configurato, maggiore di 8) caratteri aggiuntivi nella password:
    - nome o cognome dell'utente;
    - login dell'utente;
    - qualsiasi parola contenuta nel nome dell'organizzazione dell'utente che superi i tre caratteri;
    - numero di telefono e fax dell'utente o dell'organizzazione;
    - indirizzo e-mail dell'utente.

1.12. Misure Integrate

Per impedire attacchi "brute-force" sulle password, un algoritmo di throttling limita i tentativi di indovinare le password. I Clienti possono configurare la loro policy sulle password come segue:

- lunghezza minima della password (superiore a 8 caratteri);
- obbligo di utilizzare lettere maiuscole e minuscole nella password;
- obbligo di utilizzare numeri nella password;
- obbligo di utilizzare simboli nella password;
- obbligo di utilizzare numeri o simboli nella password;
- scadenza della password dopo un determinato numero di giorni;
- blocco degli account utente dopo un determinato numero di tentativi di inserimento della password.

Per impostazione predefinita, la password minima si compone di 8 caratteri e non può essere ridotta. Le altre impostazioni, in conformità con le migliori prassi recenti, non sono predefinite, ma possono essere configurate da Infor Nexus per le organizzazioni dei Clienti come parte dell'implementazione.

1.13. Software Dannoso

Infor si avvale di software anti-malware/antivirus standard generalmente accettati dal settore. Per quanto possibile, utilizza funzioni di protezione quasi in tempo reale al fine di fornire i Servizi Cloud senza “time bombs”, “worm”, “virus”, “Trojan horse”, “codici di protezione”, “chiavi di distruzione dati” o altri programmi volti a modificare, cancellare, danneggiare, disattivare o disabilitare i Dati del Cliente o a impedire o limitare l’accesso del Cliente ai Dati del Cliente.

1.14. Sicurezza Fisica

Le strutture che contengono i Sistemi dovranno:

i. essere strutturalmente progettate per resistere alle intemperie e ad altre condizioni naturali ragionevolmente prevedibili;

ii. disporre di adeguate protezioni fisiche ambientali per aiutare a proteggere i Sistemi da danni legati a fumo, calore, acqua, fuoco, umidità o fluttuazioni dell’energia elettrica;

iii. essere supportate da sistemi di generazione di energia di back-up in loco; e

iv. essere sottoposte a controlli adeguati per garantire che solo il personale autorizzato abbia accesso fisico alla struttura.

2. Audit

2.1 Diritti di Audit

Nell’ambito del programma di supervisione del fornitore, il Cliente e (se applicabile) l’ente regolatorio competente possono richiedere, una volta all’anno, sotto forma di audit via posta (ossia un questionario basato sulla certificazione ISO 27001), la documentazione che dettagli la procedura adottata da Infor in base al suo programma per la sicurezza delle informazioni, i relativi processi e controlli. Infor riconosce che, nella misura in cui tale documentazione sia prontamente disponibile, fornirà quanto ragionevolmente richiesto dal Cliente, purché ciò non (a) metta a repentaglio la riservatezza, l’integrità o la disponibilità dei dati o dei servizi degli altri clienti di Infor o (b) violi la riservatezza, l’integrità e la disponibilità dei dati o dei servizi di terzi che forniscono Servizi al Cliente per conto di Infor. La documentazione fornita da Infor non includerà prove (tra cui, a mero titolo esemplificativo, la prova della formazione, la prova dei test, i risultati delle valutazioni sui rischi). Infor risponderà al questionario entro 30 giorni. Se questo termine non può essere rispettato, Infor collaborerà con il Cliente per concordare a un lasso di tempo ragionevole per l’invio del questionario. Tale documentazione deve essere considerata un’Informazione Riservata di Infor. Infor non prenderà in considerazione i rilievi dei Clienti derivanti da questo audit via posta.

2.2 Audit di terze parti

Una volta ogni 12 mesi durante il Periodo di Abbonamento, Infor dovrà, a proprie spese, incaricare un revisore indipendente debitamente qualificato per condurre una revisione della progettazione e dell’efficacia operativa degli obiettivi di controllo definiti da Infor e delle attività di controllo in relazione ai Servizi Cloud (escluso il Supporto). Infor farà in modo che tale revisore prepari un report SOC II Tipo 2 per tutti i Servizi Cloud e, solo per i Servizi Cloud multi-tenant, un rapporto SOC II Tipo 2 e, se applicabile, SOC I Tipo 2 per i Servizi Cloud (collettivamente, l’“Audit Report”). L’Audit Report è un’Informazione Riservata di Infor, ma è disponibile per il Cliente sul portale di- assistenza di Infor. Il Cliente può condividere una copia di tale Audit Report con i propri revisori e con le autorità di regolamentazione, a condizione che i revisori e le autorità di regolamentazione siano informati che tale Audit Report è un’Informazione Riservata di Infor e deve essere protetta di conseguenza.

3. Gestione delle Modifiche per i Servizi Cloud

Infor segue un processo di controllo delle modifiche che regola l’identificazione e l’implementazione delle modifiche all’interno delle risorse tramite cui vengono prestati i Servizi Cloud di Infor al fine di evitare modifiche indesiderate al codice sorgente delle applicazioni, alle interfacce, ai sistemi operativi o le modifiche di back-end dei dati all’interno di campi e tabelle esistenti. Tutte le modifiche richieste alle risorse per la prestazione dei Servizi Cloud di Infor devono seguire un processo di controllo delle modifiche di implementazione. Infor documenta e conserva un registro dettagliato che attesta la propria conformità a questo processo, come ad esempio tramite un sistema di ticketing, e le registrazioni delle

procedure di test per qualsiasi modifica, compresi, a mero titolo esemplificativo, la data e l'ora di ogni modifica e una descrizione della natura della modifica.

4. Segregazione dei Dati; Assenza di Sfruttamento

4.1 Segregazione

I Dati sono tenuti logicamente separati dai dati di Infor e dai dati di qualsiasi altro cliente di Infor mediante l'adozione di mezzi tecnici appropriati.

4.2 Assenza di Sfruttamento, Statistiche Aggregate

I Dati sono Informazioni Riservate del Cliente e il Cliente è titolare di tutti i diritti sui propri Dati. Infor non sfrutterà commercialmente i Dati e non accederà ai Dati se non nella misura necessaria per eseguire i Servizi Cloud e per adempiere alle proprie obbligazioni in conformità al Contratto.

Per quanto riguarda i Dati, Infor può raccogliere Statistiche Aggregate, che sono di esclusiva proprietà di Infor e non possono essere considerate Dati del Cliente. Le "Statistiche Aggregate" sono dati statistici e informazioni sulle prestazioni, riguardanti l'uso e il funzionamento dei Servizi da parte del Cliente, generati attraverso sistemi di strumentazione e registrazione.

5. Gestione delle risorse

Infor adotta un processo formale di gestione delle risorse che prevede il mantenimento di:

i. un inventario delle risorse utilizzate per fornire i Servizi ("Risorse"), volto a identificare e stabilire chiaramente la proprietà e il controllo delle Risorse;
ii. procedure volte a gestire la restituzione, la distruzione o la rimozione dei Dati dalle Risorse in questione; e
iii. procedure progettate per proteggere le Risorse da minacce e vulnerabilità, interne o esterne, intenzionali o accidentali.

6. Scansione delle Vulnerabilità e Test di Penetrazione

Infor si avvale di un processo di gestione delle vulnerabilità per individuare i rischi derivanti dallo sfruttamento di difetti o debolezze accertati o identificati che potrebbero essere sfruttati (accidentalmente o intenzionalmente) e provocare danni o accessi non autorizzati ai Sistemi ("Vulnerabilità"). Infor gestirà le Vulnerabilità entro le tempistiche standard di settore generalmente accettate. Infor dovrà porre rimedio o limitare le Vulnerabilità in modo commisurato al rischio che tali Vulnerabilità rappresentano, secondo il quadro definito da Infor, in coerenza con gli standard di settore generalmente accettati.

Annualmente, Infor incarica, a proprie spese, una terza parte indipendente per condurre test di penetrazione nei Servizi Cloud multi-tenant, compresi test manuali umani, per valutare i controlli di sicurezza dei Sistemi secondo metodologie standard di settore generalmente accettate.

Per i Servizi Cloud multi-tenant, le valutazioni dei test di sicurezza, comprese le scansioni del codice sorgente e le scansioni delle Vulnerabilità vengono condotte prima del rilascio del codice e durante tutto il ciclo di vita del prodotto dei Servizi Cloud (ovvero, negli ambienti di sviluppo e produzione) con la finalità di identificare potenziali Vulnerabilità da correggere o mitigare. Su base annuale viene eseguito il test di penetrazione sui Servizi Cloud multi-tenant per identificare le Vulnerabilità da correggere o mitigare.

7. Risposta agli Incidenti sulla Sicurezza delle Informazioni

Se Infor viene a conoscenza del fatto che i Dati sono stati, o si prevede ragionevolmente che siano stati, oggetto di un uso o di una divulgazione non autorizzata dal presente Contratto (un "Incidente sulla Sicurezza delle Informazioni"), Infor dovrà: (i) comunicare tempestivamente e senza ritardi ingiustificati (e in ogni caso entro 48 ore dal momento in cui Infor viene a conoscenza di tale Incidente di Sicurezza delle Informazioni) al Cliente interessato il verificarsi di tale Incidente sulla Sicurezza delle Informazioni; (ii) indagare e condurre un'analisi ragionevole della/e causa/e di tale Incidente sulla Sicurezza delle Informazioni; (iii) fornire aggiornamenti periodici di qualsiasi indagine in corso al Cliente; (iv) sviluppare e implementare un piano appropriato per rimediare alla causa di tale Incidente sulla Sicurezza delle Informazioni nella misura in cui tale causa rientri nel controllo di Infor; e (v) cooperare con le ragionevoli

indagini del Cliente o con gli sforzi del Cliente per rispettare qualsiasi notifica o altri requisiti normativi applicabili a tale Incidente sulla Sicurezza delle Informazioni. Su richiesta del Cliente e a spese del Cliente, in caso di un Incidente sulla Sicurezza delle Informazioni, Infor consegnerà (nella misura consentita dalla legge e fatte salve le adeguate protezioni di riservatezza) le copie dei registri delle attività dei Sistemi applicabili (esclusivamente in relazione all'Incidente sulla Sicurezza delle Informazioni che riguarda il Cliente) al Cliente per utilizzare le stesse in qualsiasi procedimento legale o regolamentare del Cliente o in qualsiasi indagine governativa del Cliente.

8. Registrazione e Monitoraggio

Infor monitora le risorse utilizzate per fornire i Servizi Cloud attraverso una serie di strumenti, specificamente configurati per gestire i log e gli avvisi. I registri vengono conservati fisicamente e sono virtualmente protetti per prevenirne la manomissione. Le informazioni sensibili e le password non vengono in nessun caso registrate. Oltre ad acquisire informazioni relative ai Servizi, gli strumenti di monitoraggio consentono agli amministratori di tenere traccia dell'attività degli utenti in ingresso e in uscita dal Sistema.

9. Sicurezza delle Risorse Umane e Formazione

Il personale di Infor che eroga i Servizi Cloud è soggetto a obblighi di riservatezza, è a conoscenza delle minacce e dei problemi di sicurezza delle informazioni, riceve una formazione generale sulla sicurezza almeno una volta all'anno ed è in grado di sostenere le politiche di sicurezza sulle informazioni dell'organizzazione in generale e nell'ambito delle proprie specifiche funzioni lavorative.

10. Controlli sui Dispositivi Endpoint (pc portatili, postazioni di lavoro e Dispositivi Mobili di Infor)

Infor implementa misure di sicurezza generalmente accettate dal settore per la protezione degli endpoint, tra cui l'automazione della gestione delle patch delle applicazioni e dei sistemi operativi e la protezione antivirus.

11. Restituzione dei Dati

11.1 Restituzione

Il Cliente ha accesso ai propri dati per tutta la durata dell'abbonamento, ad eccezione dei tempi di inattività programmati, della manutenzione di emergenza e di quanto previsto in altre linee guida sulla disponibilità dei livelli di servizio. Qualora il Cliente richieda la restituzione dei Dati del Cliente in un formato non standard o richieda qualsiasi altro servizio di assistenza in sede di cessazione del rapporto contrattuale, Infor e il Cliente dovranno concordare l'ambito di tali servizi di assistenza in sede di cessazione del rapporto contrattuale e gli importi dovuti a titolo di compenso e spese per tali servizi. Fermo quanto sopra, i Dati Condivisi devono rimanere sulla Piattaforma Infor Nexus in quanto non sono di esclusiva proprietà del Cliente, ma sono condivisi. Per "Dati Condivisi" si intendono tutti i dati visibili sia al Cliente/Utente sia a uno o più utenti autorizzati aggiuntivi sulla Infor Nexus Platform, come ad esempio fornitori e service provider. L'archiviazione dei Dati avviene a livello della transizione e non del Cliente.

11.2 Distruzione

I Dati forniti a Infor ai fini della prestazione del Supporto (ad esempio, tramite un ticket di Supporto registrato sul portale di Supporto) vengono eliminati cinque anni dopo la data di chiusura del ticket dell'incidente. Il nome del Cliente e le sue informazioni di contatto (ad es. indirizzo e-mail dell'utente, nome e numero di telefono dell'utente) utilizzate per gestire il ciclo di vita dei ticket di Supporto vengono disattivate e resi anonimi al termine del Supporto.

12. Subappaltatori

I subappaltatori di Infor, che forniscono beni e servizi a Infor in relazione ai Servizi Cloud di Infor, forniranno tali beni e servizi a condizioni sostanzialmente simili a quelle stabilite nel presente ISP. Prima di incaricare un subappaltatore terzo per l'esecuzione di uno qualsiasi dei Servizi Cloud ai sensi del presente ISP, Infor controllerà tale terza parte con ragionevole diligenza al fine di garantire che tale terza parte possa rispettare gli obblighi di riservatezza e sicurezza ai sensi del presente ISP. Infor è responsabile per tutto quanto svolto dai propri subappaltatori nell'ambito dei Servizi Cloud.