

Piano per la Sicurezza delle Informazioni

Oggetto: Il presente Piano per la Sicurezza delle Informazioni (Information Security Plan, “ISP”) deve considerarsi incorporato negli accordi che il Cliente conclude con Infor (collettivamente, gli “Accordi”). In caso di conflitto o incoerenza tra le condizioni del presente ISP e qualsiasi altra condizione 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, riguardo in via generale a tutti i Clienti:

- i. l’hardware, le attrezzature e la configurazione software dei sistemi per cui Infor fornisce:
 - a. Servizi Cloud (per chiarezza, i Servizi Cloud includono il Supporto);
 - b. Servizi Professionali; e
 - c. Supporto riguardo al Software On Premises

(i predetti hardware, attrezzature e la configurazione software dei sistemi sono di seguito denominati collettivamente nel presente ISP i “Sistemi” e i Servizi Cloud, i Servizi Professionali e il Supporto per il Software-On Premises sono di seguito denominati collettivamente i “Servizi”), inoltre

- ii. I dati del Cliente forniti a Infor, sia:
 - o come Dati del Cliente o,
 - 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: Termini in maiuscolo utilizzati nel presente ISP e non definiti all’interno dello stesso hanno il significato attribuito loro nel Contratto Software stipulato tra Infor ed il Cliente in questione (il “Contratto”).

Esclusioni: Il presente ISP non è applicabile: (i) agli accordi per i Servizi Professionali di Infor in base ai quali il Software On—Premises del Cliente è ospitato da Infor in base a un contratto di Servizi Professionali negoziato separatamente, o (ii) 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 una descrizione del lavoro, Ed 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 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 avrà la facoltà di 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 analogica; (ii) non meno rigorose degli standard di settore generalmente accettati; e (iii) richieste dalle leggi applicabili. Infor non si assume responsabilità nei riguardi di sistemi operativi, prodotti e servizi di terzi che interagiscono con i Sistemi e che il Cliente (a) ha sviluppato per se stesso, o (b) concede in licenza in base a proprie condizioni di licenza a terzi.

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 senza limitazioni 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" per la prestazione dei Servizi. Infor conserva e aggiorna un registro di tale personale. Tale 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.
- iv. Infor disattiva gli account dei propri dipendenti dalle applicazioni o dagli archivi di dati che contengono i Dati quando per tali dipendenti cessa il rapporto di lavoro o sono 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 alcun Sistema. Infor impone, su tutti i Sistemi Infor, l'uso di "password forti" richieste dal sistema, secondo le migliori prassi del 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 un determinato numero di tentativi consecutivi 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/prevenzione delle intrusioni (intrusion detection system "IDS" e intrusion prevention system "IPS") per monitorare i propri Sistemi e le proprie procedure contro le violazioni della sicurezza, infrazioni e attività sospette. Ciò include attività esterne sospette (tra cui, a mero titolo esemplificativo e non esaustivo, sonde non autorizzate, scansioni o tentativi di intrusione) e attività interne sospette (tra cui, a mero titolo esemplificativo e non esaustivo, 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 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

- Nel transito su reti pubbliche, i Dati sono criptati, almeno, con TLS 1.2 o il suo successore logico.
- Quando i Dati sono inattivi all'interno dei Sistemi, i Dati sono criptati, almeno, con AES 256 bit o il suo successore logico (ad eccezione degli interventi di Supporto di risoluzione incidenti per le soluzioni della piattaforma IBM i Series o Z rivendute da Infor).

1.7. Gestione dell'Identità

Infor utilizza un modello di sicurezza condiviso per allocare la responsabilità sulla gestione dell'identità. Infor è in grado di associare le applicazioni dei Sistemi al fornitore dei servizi di gestione delle identità del Cliente per l'autenticazione.

1.8. Software Dannoso

Infor si avvale di software anti-malware/antivirus standard e generalmente accettati dal settore. Per quanto possibile, Infor utilizza funzioni di protezione quasi in tempo reale con l'intento di fornire i Servizi Cloud o Servizi On-Premises privi di "time bombs", "worms", "virus", "Trojan horses", "codici di protezione", "chiavi di distruzione dati" o altri programmi volti a (i) modificare, cancellare, danneggiare, disattivare o disabilitare i Dati dei Clienti o impedire o limitare l'accesso del Cliente ai Dati del Cliente, per quanto riguarda i Servizi Cloud; o (ii) modificare, eliminare, danneggiare o disabilitare i dati del Cliente all'interno del Software on Premises, per quanto riguarda il Software On Premises.

1.9. 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 dettaglia la procedura adottata da Infor riguardante il 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 procedurale fornita da Infor non includerà prove (tra cui, a mero titolo esemplificativo e non esaustivo, 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 detto adempimento. Tale documentazione costituirà 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 I di tipo 2 per tutti i Servizi Cloud e, solo per i Servizi Cloud ospitati in un ambiente condiviso ("multi-tenant"), un report SOC II di tipo 2 (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 tali revisori e tali autorità di regolamentazione siano informati che tale Audit Report è un'Informazione Riservata di Infor e deve essere protetta di conseguenza.

Inoltre, Infor dovrà, a proprie spese, incaricare annualmente un revisore indipendente debitamente qualificato per condurre una revisione della sicurezza delle informazioni in relazione a determinati Servizi Cloud multi-tenant indicati su trust.infor.com. e come Supporto sia del Software On-Premise che dei Servizi Cloud, in ogni caso ai sensi dello standard (ISO) 27001 dell'Organizzazione Internazionale per la Standardizzazione. Infor farà in modo che tale revisore prepari un report in conformità a tale standard. L'Audit Report non sarà disponibile al Cliente. Tuttavia, il Cliente potrà ottenere in qualsiasi momento una copia del certificato risultante dal sito di sicurezza cloud di Infor (trust.infor.com). Il certificato identificherà il Software che è oggetto del report. Nell'ambito di questa certificazione ISO 27001, Infor conserva un manuale sul Sistema di Gestione della Sicurezza delle Informazioni (Information Security Management System) per il Software incluso nella certificazione e il relativo Supporto, che contribuisce a garantire la protezione, la riservatezza, l'integrità e la disponibilità delle risorse di Infor utilizzate per fornire tali Servizi.

Ulteriori certificazioni di terze parti sono disponibili all'indirizzo trust.infor.com.

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'ambito delle risorse addette alla fornitura dei Servizi Cloud di Infor al fine di evitare modifiche indesiderate al codice sorgente delle applicazioni, interfaccia, sistemi operativi o modifiche di back-end dei dati all'interno di campi e tabelle esistenti. Tutte le modifiche richieste alle risorse addette alla prestazione dei Servizi Cloud di Infor devono seguire una procedura di controllo delle modifiche di implementazione. Infor documenta e conserva un registro dettagliato che attesta la propria conformità a questa procedura, come ad esempio un sistema di ticketing, e le registrazioni delle procedure di verifica per qualsiasi modifica, compresi, a mero titolo esemplificativo e non esaustivo, la data e l'ora di effettuazione di ciascuna 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 e per adempiere alle proprie obbligazioni in conformità al Contratto.

Infor raccoglie dati statistici e informazioni di prestazione, generati con strumentazioni e sistemi di registrazione, riguardanti l'utilizzo e l'operatività dei Servizi da parte dei Clienti ("Statistiche Aggregate").Le Statistiche Aggregate sono di proprietà esclusiva di Infor e non possono essere considerati Dati.

5. Gestione delle Strumentazioni

Infor ha adottato una procedura formale di gestione delle strumentazioni che prevede il mantenimento di:

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

6. Scansione delle Vulnerabilità e Test di Penetrazione

Infor si avvale di una procedura 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 tempistiche standardizzate generalmente accettate nel settore. 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 ospitato in un ambiente multi-tenant, ivi inclusi test manuali umani per valutare i controlli di sicurezza dei Sistemi secondo metodologie standard di settore generalmente accettati.

Per il Software di Sottoscrizione 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 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 autorizzati 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 sulla 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 al Cliente aggiornamenti periodici su qualsiasi indagine in corso; (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 nell’ambito di controllo di Infor; e (v) cooperare con il Cliente nelle sue ragionevoli indagini e sforzi 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 procedura 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 attraverso una serie di strumenti, specificamente configurati per gestire le registrazioni 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 al Servizio, gli strumenti di monitoraggio consentono agli amministratori di tenere traccia dell’attività degli utenti in ingresso e in uscita dal Sistema.

9. Sicurezza e Formazione delle Risorse Umane

Il personale di Infor che fornisce i Servizi 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 sia in generale che nell’ambito delle proprie specifiche funzioni lavorative.

10. Controllo sui Dispositivi Endpoint (Pc Portatili, Postazioni di Lavoro e Dispositivi Mobili di Infor)

Infor applica 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 e Distruzione dei Dati

11.1. Restituzione

In caso di risoluzione o alla scadenza dei Servizi Cloud, Infor metterà prontamente (entro 3-5 giorni lavorativi dal ricevimento della richiesta scritta del Cliente mediante un ticket di Supporto standard, la richiesta dovendo essere effettuata entro 30 giorni dalla data di risoluzione (10 giorni per i single-tenant) a disposizione del Cliente tutti i Dati del Cliente sotto forma di esportazione nativa del database fornita tramite il servizio di trasferimento sicuro dei file di Infor. Qualora il Cliente richieda la restituzione dei Dati del Cliente in un formato alternativo o

richieda qualsiasi altro servizio di assistenza a causa della risoluzione, Infor e il Cliente dovranno concordare reciprocamente l'ambito di tali servizi di assistenza e i corrispettivi e le spese dovuti per tali servizi di assistenza. Prima della risoluzione, il Cliente ha accesso ai Dati del Cliente tramite le interfacce dell'applicazione e Infor dovrà restituire al Cliente, su richiesta di quest'ultimo effettuata attraverso il portale di Supporto, copie dei backup dei dati fino a due volte ogni 12 mesi quale esportazione nativa del database tramite il servizio di Infor di trasferimento sicuro dei file. Ulteriori richieste saranno a pagamento.

Inoltre, per chiarezza, la restituzione o la distruzione dei Dati Personali avverrà in conformità ai termini e condizioni dell'Accordo Sulla Protezione dei Dati.

I dati per i sistemi di resa (es. Gestione dei Documenti di Infor, EzRMS di Infor o l'Ottimizzatore dei Prezzi per l'Accoglienza di Infor) saranno cancellati al momento della risoluzione e non saranno trasferiti al Cliente.

11.2. Distruzione

Fatta eccezione per l'Assistenza sulla Transizione richiesta dal Cliente, Infor cancellerà definitivamente tutte le istanze (online o accessibili in rete) relative ai Dati del Cliente entro 35 giorni dalla risoluzione o dalla scadenza dei Servizi Cloud in conformità con NIST 800-88.

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

12. Subappaltatori

I subappaltatori di Infor, che forniscono beni e servizi a Infor in relazione ai Servizi di Infor, forniranno tali beni e servizi a condizioni sostanzialmente analoghe a quelle stabilite nel presente ISP. Prima di ingaggiare un subappaltatore terzo per l'esecuzione di uno qualsiasi dei Servizi di cui al 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 di cui al presente ISP. Infor è responsabile di tutte le azioni dei suoi subappaltatori nell'ambito del supporto ai Servizi.

Disclaimer: i seguenti prodotti possono avere termini di sicurezza aggiuntivi o diversi: Acumen Invest (Infor Trade Promotions Management) e Acumen Radar (Infor Strategic Pricing Management) Anael (SaaS) (Francia); 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).