Piano per la Sicurezza delle Informazioni

BPCS/LX, XA, Sistema 21

REVISIONI IN VIGORE NOVEMBRE 2024

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 di cui Infor si avvale per prestare:
- Servizi Cloud (per chiarezza, i Servizi Cloud includono il Supporto)
- Servizi Professionali, e
- Supporto del Software On Premises

(tutto l'hardware, le apparecchiature e le configurazioni del software sono di seguito denominati collettivamente nel presente ISP come i "Sistemi" e i Servizi Cloud, i Servizi Professionali e il Supporto Software On Premises sono di seguito denominati collettivamente i "Servizi");

(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 stipulato tra Infor ed il Cliente in questione (il "Contratto").

Esclusioni: Il presente ISP non è applicabile: (i) agli accordi di Servizi Professionali di Infor nei quali il Software On Premises del Cliente è ospitato da Infor in base ad un Contratto di Servizi Professionali negoziato separatamente, o (ii) nel caso in cui Infor esegua 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* e, 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 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.

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 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 delle intrusioni/sistema di prevenzione delle intrusioni (IDS/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, 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 di una tecnologia firewall di rete progettata per proteggere la connettività e gli ambienti ospitati che sono accessibili da Internet.

1.5. Aggiornamenti

Infor mantiene i Sistemi aggiornati con upgrade, aggiornamenti, correzioni di bug e nuove versioni. Gli aggiornamenti, gli upgrade e le correzioni dei sistemi operativi e delle applicazioni vengono concordati e programmati con il Cliente.

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 nell'ambito di Servizi Cloud, 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 allocare la responsabilità sulla gestione dell'identità sicurezza. Infor è in grado di associare le applicazioni dei Sistemi al fornitore dei servizi di gestione delle identità del Cliente.

1.8. 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 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 I Tipo 2 per tutti i Servizi Cloud e, solo per i Servizi Cloud multi-tenant, un rapporto SOC II Tipo 2 (collettivamente, il "Rapporto di audit") (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 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 possiede 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. Sono compresi test manuali umani, per valutare i controlli di sicurezza dei Sistemi secondo metodologie standard di settore generalmente accettati.

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 sui Servizi Cloud multi-tenant e single-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 sia stati, oggetto di un uso o di una divulgazione non autorizzati dal Contratto (un "Incidente sulla Sicurezza delle Informazioni"), Infor dovrà: (i) notificare 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 al Cliente aggiornamenti periodici di 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 nel controllo di Infor; e (v) cooperare con il Cliente e le 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 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 e Formazione delle Risorse Umane

Il personale di Infor che presta 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 dei 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 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) 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 in sede di risoluzione, Infor e il Cliente dovranno concordare reciprocamente l'ambito di tali servizi di assistenza e dovranno altresì concordare 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 inviata tramite 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 soggette a corrispettivo.

Inoltre, per chiarezza, la restituzione o la distruzione dei Dati Personali avverrà in conformità con i termini dell'Accordo sulla Protezione dei Dati.

11.2 Distruzione

Fatta eccezione per l'Assistenza di 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 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, nome e numero di telefono dell'utente) utilizzate per gestire il ciclo di vita dei ticket di Supporto vengono disattivati al termine del Supporto e vengono eliminati su richiesta del Cliente.

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 ingaggiare 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 di tutte le azioni dei suoi subappaltatori nell'ambito del supporto dei Servizi Cloud.