Piano per la Sicurezza delle Informazioni

Revenue Managementt System (SaaS)

Il presente Piano per la Sicurezza delle Informazioni (Information Security Plan, "ISP") è allegato al Modulo d'Ordine tra Infor e il Cliente ivi indicato e stabilisce le attuali misure di sicurezza di Infor, le quali sono progettate per salvaguardare l'hardware, le attrezzature e la configurazione software dei sistemi (i) su cui Infor supporta l'uso del Software in Abbonamento (indicato nel Modulo d'Ordine) e i relativi Servizi in Abbonamento e (ii) in cui i Dati del Cliente sono stati forniti, inseriti o caricati per essere utilizzati da o con il Software in Abbonamento, dal Cliente o dai suoi Utenti Autorizzati (i e ii collettivamente, i "Sistemi"). Per chiarezza, i termini in maiuscolo utilizzati nel presente ISP e non definiti all'interno dello stesso hanno il significato attribuito loro nel Contratto di Software as a Service stipulato tra Infor ed il Cliente in questione (il "Contratto"). Il presente ISP non è applicabile agli accordi di servizio gestito di Infor, nei quali il software on-premise del Cliente è ospitato da Infor in base ad un contratto di servizi professionali negoziato separatamente.

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 del Cliente.

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 del Cliente che Infor tratta su richiesta del Cliente. Dette misure di sicurezza sono: (i) non meno rigorose di quelle adottate da Infor per le proprie informazioni di natura simile; (ii) non meno rigorose degli standard di settore generalmente accettati; e (iii) richieste dalle leggi applicabili.**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 di accesso ai Dati del Cliente, che includono le seguenti misure:

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

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

iii. Infor istruisce il personale che ha accesso ai Dati del Cliente 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 del Cliente quando tali dipendenti vengono licenziati o trasferiti oppure quando non hanno più la necessità di accedere a tali Dati del Cliente. Infor rivede regolarmente l'elenco delle persone e dei servizi che hanno accesso ai Dati del Cliente 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 altri parametri di sicurezza su nessun Sistema. Infor impone l'uso di "password forti" richieste dal sistema, secondo le best practice di settore generalmente accettate su tutti i Sistemi Infor. Infor richiede che tutte le password e le credenziali di accesso siano mantenute riservate e non vengano condivise tra il personale, e 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 del Cliente quando un account supera più un determinato numero di tentativi consecutivi di inserimento di una password errata.

vii. L'accesso remoto ai Sistemi che contengono i Dati del Cliente tramite Infor CloudOps richiede un'autenticazione a due fattori (ad esempio, richiede almeno due fattori separati 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. Questo sistema 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 del Cliente). Infor esamina regolarmente i registri degli accessi alla ricerca di segnali di comportamenti dannosi o di accessi non autorizzati.

1.4. Firewall

Infor dispone di una tecnologia firewall di rete progettata per proteggere i Dati del Cliente 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 del Cliente sono criptati, almeno, con TLS 1.2 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. Software Dannoso

Infor si avvale di software anti-malware/antivirus standard generalmente accettati dal settore e, per quanto possibile, utilizza funzioni di protezione quasi in tempo reale per fornire il Software in Abbonamento e i Servizi in Abbonamento che non contengano "time bombs", "worm", "virus", "Trojan horse", "codici di protezione", "chiavi di distruzione dei dati" o altri dispositivi di programmazione destinati ad accedere, modificare, cancellare, danneggiare, disattivare o disabilitare i Dati del Cliente o a impedire o limitare l'accesso del Cliente ai Dati del Cliente ("Codice Dannoso").

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. avere adeguate protezioni fisiche ambientali per aiutare a proteggere i Sistemi da danni legati a fumo, calore, acqua, fuoco, umidità o fluttuazioni della potenza elettrica;

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

iv. avere 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 di normazione possono richiedere, una volta all'anno, sotto forma di audit via posta (ossia un questionario basato sulla certificazione ISO 27001), la documentazione procedurale di Infor riguardante il suo programma per la sicurezza delle informazioni, i processi e i controlli. Infor riconosce che, nella misura in cui tale documentazione procedurale sia prontamente disponibile, fornirà la documentazione ragionevolmente richiesta dal Cliente, purché tale documentazione 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 in Abbonamento al cliente per conto di Infor. La documentazione procedurale 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 raggiungere un accordo per il completamento del questionario. Tutta questa 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 ogni12 mesi durante il Periodo di validità dell'Abbonamento, Infor dovrà, a proprie spese, incaricare un revisore indipendente debitamente qualificato di condurre una revisione del progetto e dell'efficacia operativa degli obiettivi di controllo definiti da Infor e delle attività di controllo in relazione ai Servizi in Abbonamento. Infor farà in modo che tale revisore prepari una relazione in conformità con loStatement on Standards for Attestation Engagements n. 18 (SSAE 18) dell'American Institute of Certified Public Accountants o con uno standard equivalente, che può includere ISAE 3402 (la "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 autorità di regolamentazione, a condizione che i revisori e le autorità di regolamentazione siano informati che tale Audit Reportè un'Informazione Riservata di Infor e deve essere protetta di conseguenza.

Inoltre, una volta ogni 12 mesi durante il Periodo di validità dell'Abbonamento, Infor dovrà, a proprie spese, incaricare un revisore indipendente debitamente qualificato di condurre una revisione della sicurezza delle informazioni in relazione ai Servizi in Abbonamento per determinati Software in Abbonamento multi-tenant indicati su trust.infor.com ai sensi della certificazione ISO27001. Infor farà in modo che tale revisore prepari una relazione in conformità agli standard ISO 27001 dell'Organizzazione internazionale per la standardizzazione. L'Audit Report non sarà disponibile al Cliente; tuttavia il Cliente può ottenere una copia del certificato risultante dal sito di sicurezza cloud di Infor (trust.infor.com) in qualsiasi momento. Il certificato identificherà il Software in Abbonamento 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 in Abbonamento incluso nella certificazione e i relativi Servizi in Abbonamento, che contribuisce a garantire la protezione, la riservatezza, l'integrità e la disponibilità delle risorse di Infor utilizzate per fornire tali Servizi in Abbonamento.

Infor segue un processo di controllo delle modifiche che regola l'identificazione e l'implementazione delle modifiche all'interno delle risorse di fornitura dei Servizi in Abbonamento di Infor per evitare modifiche indesiderate al codice sorgente delle applicazioni, alle interfacce, ai sistemi operativi o le modifiche di back-end ai dati all'interno di campi e tabelle esistenti. Tutte le modifiche richieste alle risorse per la fornitura dei Servizi in Abbonamento di Infor devono seguire un processo di controllo delle modifiche di implementazione. Infor documenta e conserva un registro dettagliato della sua conformità a questo processo, come ad esempio 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.

3.Nessun tipo di sfruttamento; Statistiche Aggregate

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

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, generate attraverso sistemi di strumentazione e registrazione, riguardanti l'uso e il funzionamento del Software in Abbonamento e dei Servizi in Abbonamento da parte del Cliente.

4 Gestione delle risorse

Infor possiede un processo formale di gestione delle risorse che include:

i. mantenere un inventario delle risorse utilizzate per fornire i Servizi in Abbonamento ("Risorse"), stabilire una chiara proprietà e un controllo delle Risorse, essere in grado di identificare le Risorse e di gestire la restituzione, la distruzione o la rimozione dei Dati del Cliente dalle Risorse in questione; e
ii. procedure progettate per tutelare le Risorse da minacce e vulnerabilità, interne o esterne, intenzionali o accidentali.

5 Scansione delle Vulnerabilità e Test di Penetrazione

Infor si avvale di un processo di gestione delle vulnerabilità per analizzare i rischi derivanti dallo sfruttamento di difetti o debolezze pubblicati o identificati che potrebbero essere sfruttati (accidentalmente o intenzionalmente) e causare danni o accesso non autorizzato ai Sistemi ("Vulnerabilità"). Infor si occuperà delle Vulnerabilità entro i tempi standard di settore generalmente accettati. Infor dovrà porre rimedio o limitare le Vulnerabilità in modo commisurato al rischio che tali Vulnerabilità rappresentano, secondo il quadro definito da Infor, coerente con gli standard di settore generalmente accettati.

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

Per alcuni Software in Abbonamento 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 per tutto il ciclo di vita del prodotto del Software in Abbonamento (ovvero, negli ambienti di sviluppo e produzione) con la finalità di identificare potenziali Vulnerabilità da correggere o mitigare. Il

test di penetrazione annuale viene eseguito su alcuni Sistemi multi-tenant per identificare le Vulnerabilità da correggere o mitigare.

6 Risposta agli Incidenti sulla Sicurezza delle Informazioni

Se Infor viene a conoscenza che i Dati del Cliente sono stati, o si prevede ragionevolmente che siano, oggetto di un uso o di una divulgazione non autorizzati con il presente ISP (un "Incidente di Sicurezza delle Informazioni"), Infor dovrà: (i) notificare tempestivamente e senza ritardi ingiustificati (e in ogni caso entro 48 ore dal momento in cui viene a conoscenza di tale Incidente di Sicurezza delle Informazioni)al Cliente il verificarsi di tale Incidente di Sicurezza delle Informazioni; (ii) indagare e condurre un'analisi ragionevole della/e causa/e di tale Incidente di 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 di 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 di Sicurezza delle Informazioni. Su richiesta del Cliente e a spese del Cliente, in caso di un Incidente di 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 di Sicurezza delle Informazioni che riguarda il Cliente) al Cliente per l'utilizzo delle stesse in qualsiasi procedimento legale o regolamentare del Cliente o in qualsiasi indagine governativa del Cliente.

7 Registrazione e Monitoraggio

Infor monitora le risorse utilizzate per fornire i Servizi in Abbonamento 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 alcun modo 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.

8 Sicurezza delle Risorse Umane

Il personale di Infor che eroga i Servizi in Abbonamento 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 delle informazioni dell'organizzazione in generale e nell'ambito delle proprie specifiche funzioni lavorative.

9 Controlli dei Dispositivi Endpoint (pc portatili, postazioni di lavoro e Dispositivi Mobili di Infor)

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

10 Restituzione e Distruzione dei Dati

10.1 Restituzione

In caso di risoluzione o alla scadenza dei Servizi in Abbonamento, qualsiasi dato presente in un sistema di raccolta verrà eliminato e non sarà trasferito al cliente. 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 in sede di risoluzione e le commissioni e le spese dovute per tali servizi di assistenza in sede di risoluzione.

10.2 Distruzione

Infor cancellerà definitivamente tutte le istanze (online o accessibili in rete) dei Dati del Cliente entro 30 giorni dalla risoluzione o dalla scadenza dei Servizi in Abbonamento. Infor utilizzerà i processi standard di settore generalmente accettati per smaltire l'hardware e i componenti fisici contenenti i Dati del Cliente. Tutte le archiviazioni sono cancellate elettronicamente (azzerate) prima di essere distribuite o rimosse dall'ambiente di produzione Infor.

11 Subappaltatori

I subappaltatori di Infor, che forniscono beni e servizi a Infor in relazione ai Servizi in Abbonamento 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 in Abbonamento 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 in Abbonamento.