Informationssicherheitsplan
BPCS/LX, XA, System 21

Geltungsbereich Dieser Informationssicherheitsplan ("ISP") ist Bestandteil der zwischen dem Kunden und Infor vereinbarten Verträge (im Folgenden zusammen die „Verträge“). Im Falle des Widerspruchs zwischen den Regelungen dieses ISP and den Verträgen, gehen die Regelungen dieses ISP vor. Dieses ISP legt die aktuellen Sicherheitsmaßnahmen von Infor dar, die dazu bestimmt sind,

i. die Hardware, Geräte und Systemsoftwarekonfiguration zu schützen, auf denen Infor Cloud Services (zur Klarstellung, Cloud Services umfassen auch Support), Professionelle Dienstleistungen und Support in Bezug auf On Premises Software, erbringt. Diese Hardware, Geräte und Systemsoftwarekonfiguration werden im Rahmen dieses ISP zusammen als "Systeme" bezeichnet. Die Cloud Services, Professionellen Dienstleistungen und der On Premises Software Support werden im Rahmen dieses ISP zusammen als "Services" bezeichnet.

ii. die Kundendaten zu schützen, die Infor übermittelt wurden, entweder:

- als Kundendaten im Sinne der Definition des Vertrages
- als Daten, die Infor übermittelt wurden, zum Zwecke der Erbringungen von Professionellen Dienstleistungen und/ oder Support

(Alle diese Daten (d.h. ii.) werden im Rahmen dieses ISP gemeinsam als „DATEN“ bezeichnet.)

Definitionen: Die in diesem ISP verwendeten und hier nicht definierten Begriffe haben die Bedeutung, die diesen Begriffen in dem Software Vertrag zwischen Infor und dem Kunden (der "Vertrag") gegeben wird.

Ausnahmen: Dieser ISP gilt nicht für: (i) Professionelle Dienstleistungen durch Infor auf Grundlage eines separaten Dienstleistungsvertrages, die das Hosting von On Premises Software des Kunden zum Gegenstand haben, oder (ii) wenn Infor Dienstleistungen am Standort des Kunden erbringt und/ oder Zugriff auf die Systeme des Kunden hat. In diesen Fällen wird Infor die organisatorischen, technischen und physischen Vorgaben des Kunden einhalten, sofern in einem Statement of Work vereinbart. Der Kunde ist in diesen Fällen verantwortlich nach seinem Ermessen Infor Mitarbeiter im erforderlichen Umfang mit Nutzerautorisierung und Passwörtern zu seinen Systemen auszustatten, beziehungsweise erforderlichenfalls diese wiederum zu löschen.

Aktualisierungen: Sicherheitsbedrohungen und die Maßnahmen zum Schutz vor diesen Sicherheitsbedrohungen entwickeln sich ständig weiter. Infor kann diesen ISP jederzeit ohne Benachrichtigung des Kunden ändern, vorausgesetzt, dass Infor insgesamt ein vergleichbares oder besseres Sicherheitsniveau für die Systeme und die DATEN aufrechterhält.

1. Allgemeine Sicherheitsstandards

Infor unterhält administrative, technische und physische Sicherheitsvorkehrungen zum Schutz vor Zerstörung, Verlust, unbefugtem Zugriff oder Veränderung der Systeme und der DATEN, die (i) nicht weniger streng sind als diejenigen, die Infor für seine eigenen Informationen ähnlicher Art unterhält, (ii) nicht weniger streng sind als allgemein anerkannte Industriestandards und (iii) von den geltenden Gesetzen gefordert werden.

1.1 Sicherheitsbeauftragte

Infor hat einen oder mehrere Sicherheitsbeauftragte ernannt, die für die Koordinierung und Überwachung der Sicherheitsmaßnahmen in diesem ISP verantwortlich sind.

1.2. Zugangskontrollen

Infor kontrolliert, wer Zugang zu den DATEN erhält, u.a. durch die nachfolgend beschriebenen Maßnahmen:

i. Infor weist jeder Person mit Computerzugang zu DATEN eine eindeutige ID zu.
ii. Infor bestimmt die Mitarbeiter, die den Zugriff auf DATEN gewähren, ändern oder aufheben dürfen, und beschränkt den Zugriff auf DATEN auf der Basis des Prinzips der geringsten Berechtigung (least-privilege basis). Der Zugriff auf Daten des Kunden ist nur Mitarbeitern gestattet, die für die Bereitstellung der Services „Kenntnis haben müssen“, und Infor führt und aktualisiert eine Liste dieser Mitarbeiter. Der Zugriff auf die DATEN wird protokolliert und überwacht.
iii. Infor weist die Mitarbeiter, die Zugriff auf DATEN haben, an, administrative Sitzungen zu beenden, wenn die Computer unbeaufsichtigt sind.
iv. Infor deaktiviert die Konten von Infor-Mitarbeitern für Anwendungen oder Datenspeichern, die DATEN enthalten, wenn diese Mitarbeiter entlassen oder versetzt werden oder wenn sie keinen Zugriff mehr auf diese DATEN benötigen. Infor überprüft regelmäßig die Liste der Personen und Dienste, die Zugriff auf die DATEN haben, und entfernt Konten, die diesen Zugriff nicht mehr benötigen. Infor führt diese Überprüfung mindestens halbjährlich durch.
v. Infor verwendet auf ihren Systemen nicht die vom Hersteller vorgegebenen Standardwerte für Passwörter und andere Sicherheitsparameter. Infor schreibt die Verwendung von systemerzwungenen „starken Passwörtern“ auf allen Infor Systemen vor, die den allgemein anerkannten Best Practices der Branche entsprechen. Infor verlangt, dass alle Passwörter und Zugangsdaten vertraulich behandelt und nicht an andere Mitarbeiter weitergegeben werden. Infor deaktiviert Passwörter, von denen bekannt ist, dass sie beschädigt oder offengelegt wurden.
vi. Infor hält eine „Kontosperre“ aufrecht, indem Konten mit Zugang zu den DATEN gesperrt werden, wenn ein Konto mehr als eine definierte Zahl an aufeinanderfolgenden falschen Passworteingaben aufweist.
vii. Der Fernzugriff auf Systeme mit DATEN erfordert eine Zwei-Faktor-Authentifizierung (z. B. mindestens zwei getrennte Faktoren zur Identifizierung der Benutzer).

1.3. Erkennung und Verhinderung von Eindringlingen

Infor setzt ein Intrusion Detection System/Intrusion Prevention System (IDS/IPS) ein, um seine Systeme und seine Verfahren auf Sicherheitsverletzungen, Verstöße und verdächtige Aktivitäten zu überwachen. Dies umfasst verdächtige externe Aktivitäten (z.B. nicht autorisierter Tests, Scans oder Einbruchsversuche) und verdächtige interne Aktivitäten (z.B. nicht autorisierter Zugriff durch Systemadministratoren, nicht autorisierte Änderungen an den Systemen, Systemmissbrauch oder -diebstahl oder falsche Handhabung von DATEN). Infor überprüft die Zugriffsprotokolle regelmäßig auf Anzeichen von bösartigem Verhalten oder unbefugtem Zugriff.

1.4. Firewall

Infor hat Netzwerk-Firewall-Technologien eingerichtet und unterhält diese zum Schutz von Verbindungen und gehosteten Umgebungen, die über das Internet zugänglich sind.

1.5. Aktualisierungen

Infor hält die abonnierten Systeme mittels Upgrades, Updates, Fehlerbehebungen und neuen Versionen auf dem neuesten Stand. Aktualisierungen / Upgrades / Korrekturen von Betriebssystemen und Anwendungssystemen werden mit dem Kunden vereinbart und geplant.

1.6. Datenverschlüsselung

i. Bei der Übertragung über öffentliche Netze werden die DATEN mindestens mit TLS 1.2 oder dessen logischem Nachfolger verschlüsselt.
ii. Während sich die DATEN in Bezug auf Cloud Services, werden sie mindestens mit AES 256 Bit oder einem logischen Nachfolger verschlüsselt.

1.7. Identitätsmanagement

Infor wendet ein geteiltes Sicherheitskonzept an, um die Zuständigkeit für das Identitätsmanagement aufzuteilen. Infor ist in der Lage, die Anwendungen in den Systemen zurück an den Identitätsmanagementprovider des Kunden zum Zwecke der Authentifizierung anzubinden (Federation-Lösung).

1.8. Physische Sicherheit

Einrichtungen, die die Systeme enthalten, werden:

i. strukturell so ausgelegt sein, dass sie widrigen Witterungsbedingungen und anderen vernünftigerweise vorhersehbaren natürlichen Bedingungen standhalten;
ii. über geeignete physische Sicherheitsvorkehrungen gegen schädliche Umwelteinflüsse verfügen, um die Systeme vor Schäden durch Rauch, Hitze, Wasser, Feuer, Feuchtigkeit oder Stromschwankungen zu schützen;
iii. durch vor Ort vorhandene Notstromaggregate unterstützt werden; und
iv. über geeignete Kontrollen verfügen, die sicherstellen, dass nur befugtes Personal physischen Zugang zur Einrichtung hat.

2. Audit

2.1. Auditrechte

Im Rahmen seines Programms zur Überwachung von Dienstleistern können der Kunde und (falls zutreffend) seine staatliche Aufsichtsbehörde einmal pro Jahr in Form eines postalischen Audits (d.h. eines Fragebogens, der auf ISO 27001 basiert) eine Verfahrensdokumentation von Infor bezüglich seines Informationssicherheitsprogramms, seiner Prozesse und Kontrollen verlangen. Infor erklärt sich damit einverstanden, soweit eine solche Verfahrensdokumentation ohne wesentlichen Aufwand verfügbar ist, dem Kunden eine solche Dokumentation in angemessenem Umfang zur Verfügung zu stellen, solange diese Dokumentation nicht (a) die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten oder Diensten anderer Kunden von Infor bedroht oder (b) die Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder Diensten Dritter verletzt, die dem Kunden im Namen von Infor Services bereitstellen. Die von Infor zur Verfügung gestellte Verfahrensdokumentation enthält keine Nachweise (z.B. Schulungsnachweise, Testnachweise, Ergebnisse von Risikobewertungen). Infor wird den Fragebogen innerhalb von 30 Tagen beantworten. Falls dieser Zeitrahmen nicht eingehalten werden kann, wird Infor mit dem Kunden einen angemessenen Zeitrahmen vereinbaren. Alle diese Unterlagen sind Vertrauliche Informationen von Infor. Infor wird die Erkenntnisse des Kunden, die sich aus diesem postalischen Audit ergeben, nicht berücksichtigen.

2.2. Audit einen externen Prüfer

Einmal pro rollierenden Zwölfmonatszeitraum während der Laufzeit des Abonnements wird Infor auf eigene Kosten einen ordnungsgemäß qualifizierten unabhängigen Wirtschaftsprüfer beauftragen, eine Überprüfung der Konzeption und der operativen Wirksamkeit der von Infor definierten Kontrollziele und Kontrolltätigkeiten im Zusammenhang mit den Cloud Services (ausgenommen Support) durchzuführen. Der Prüfer wird von Infor beauftragt, einen SOC I Type 2 Bericht für die gesamten Cloud Services sowie, ausschließlich für die mandantenfähige (Multi-Tenant) Cloud Services, einen SOC II Type 2 Bericht zu erstellen (gemeinsam der "Audit Bericht"). Der Audit Bericht ist eine Vertrauliche Information von Infor. Er steht dem Kunden jedoch auf dem Infor-Supportportal zur Verfügung. Der Kunde kann eine Kopie des Audit Berichts an seine Wirtschaftsprüfer und Aufsichtsbehörden weitergeben, vorausgesetzt, die Wirtschaftsprüfer und Aufsichtsbehörden werden darüber informiert, dass der Audit Bericht zu den Vertraulichen Informationen von Infor gehört und entsprechend zu schützen ist.

3. Änderungsmanagement für Cloud Services

Infor folgt einem Änderungskontrollprozess, der die Identifizierung und Implementierung von Änderungen innerhalb der Ressourcen für die Cloud Services von Infor regelt, um unerwünschte Änderungen am Quellcode der Anwendung, an Schnittstellen, Betriebssystemen oder Back-End-Änderungen an Daten in bestehenden Feldern und Tabellen zu verhindern. Alle geplanten Änderungen an den Ressourcen für die Cloud Services müssen einen Änderungskontrollprozess für die Implementierung durchlaufen. Infor dokumentiert die Einhaltung dieses Prozesses und bewahrt detaillierte Aufzeichnungen hierüber auf, wie z.B. ein Ticket-System und Aufzeichnungen über Testverfahren für jede Änderung, einschließlich Datum und Uhrzeit einer solchen Änderung und eine Beschreibung der Art der Änderung.

4. Trennung der DATEN; keine Verwertung

4.1. Trennung

DATEN werden durch geeignete technische Mittel logisch von den Daten von Infor und den Daten anderer Infor-Kunden getrennt.

4.2. Keine Verwertung; Aggregierte Statistiken

Die DATEN sind Vertrauliche Informationen des Kunden, und der Kunde ist Inhaber aller Eigentumsrechte an seinen DATEN. Infor wird die DATEN nicht kommerziell verwerten und nur in dem Maße auf die DATEN zugreifen, wie es für die Erbringung der Services und die Erfüllung der vertraglichen Verpflichtungen erforderlich ist.

Infor kann in Bezug auf die DATEN aggregierte Statistiken sammeln, die alleiniges Eigentum von Infor sind und nicht als Kundendaten gelten. "Aggregierte Statistiken" sind statistische Daten und Leistungsinformationen, die durch Instrumentierung und Protokollierungssysteme in Bezug auf die Nutzung durch den Kunden und den Betrieb der Services generiert werden.

5. Asset-Management

Infor verfügt über einen formellen Asset-Management-Prozess, der Folgendes umfasst:

i. Führung eines Inventars der für die Erbringung der Services verwendeten Anlagen und Einrichtungen ("Assets") das dazu dient, eindeutige Eigentumsverhältnisse und Kontrolle über die Assets zu ermitteln und festzulegen;
ii. Verfahren für die Verwaltung der Rückgabe, Vernichtung oder Entfernung von DATEN aus den betreffenden Assets; und

iii. Verfahren zum Schutz von Assets vor internen oder externen, vorsätzlichen oder zufälligen Bedrohungen und Schwachstellen.

6. Scanning von Schwachstellen (Vulneribility Scan) und Penetrationstests

Infor unterhält einen Prozess des Schwachstellenmanagements, um nach Risiken zu suchen, die sich aus der Ausnutzung veröffentlichter oder erkannter Fehler oder Schwachstellen ergeben, die (versehentlich oder absichtlich) ausgenutzt werden und zu Schäden oder unberechtigtem Zugriff auf die Systeme führen könnten ("Schwachstellen"). Infor behebt Schwachstellen innerhalb allgemein anerkannter branchenüblicher Zeitrahmen. Infor wird die Schwachstellen in einer Weise beseitigen oder entschärfen, die dem Risiko entspricht, das diese Schwachstellen darstellen, und zwar in Übereinstimmung mit dem von Infor definierten Rahmen, der mit allgemein anerkannten Industriestandards übereinstimmt.

Infor beauftragt jährlich auf eigene Kosten einen unabhängigen Dritten mit der Durchführung von Penetrationstests für mandantenfähige (Multi-Tenant) Cloud Services, einschließlich manueller Tests, um die Sicherheitskontrollen der Systeme nach allgemein anerkannten Industriestandardmethoden zu bewerten.

Für mandantenfähige (Multi-Tenant) Cloud Services werden vor der Freigabe des Codes und während des gesamten Produktlebenszyklus der Cloud Services (d. h. in Entwicklungs- und Produktivumgebungen) Sicherheitstests durchgeführt, um potenzielle Schwachstellen zu ermitteln, zu beheben oder zu entschärfen. Jährlich werden Penetrationstests für mandantenfähige (Multi-Tenant) und Single-Tenant Cloud Services durchgeführt, um Schwachstellen zu identifizieren, die behoben oder entschärft werden müssen.

7. Reaktion auf Informationssicherheitsvorfälle

Wenn Infor Kenntnis davon erlangt, dass DATEN auf eine nicht durch den Vertrag autorisierten Weise genutzt oder offengelegt wurden oder eine solche Nutzung oder Offenlegung nach vernünftigen Maßstäben anzunehmen ist (ein "Informationssicherheitsvorfall"), wird Infor (i) den betroffenen Kunden unverzüglich (und in jedem Fall innerhalb von 48 Stunden nach Bekanntwerden eines solchen Informationssicherheitsvorfalls) über das Auftreten eines solchen Informationssicherheitsvorfalls benachrichtigen, (ii) eine Untersuchung durchführen und eine angemessene Analyse der Ursache(n) eines solchen Informationssicherheitsvorfalls vornehmen, (iii) den Kunden regelmäßig über die laufenden Untersuchungen informieren, (iv) einen angemessenen Plan zur Beseitigung der Ursache eines solchen Informationssicherheitsvorfalls entwickeln und implementieren, soweit diese Ursache im Einflussbereich von Infor liegt und (v) bei der angemessenen Untersuchung des Kunden oder bei den Bemühungen des Kunden um die Einhaltung etwaiger Meldevorschriften oder sonstiger auf einen solchen Informationssicherheitsvorfall anwendbarer gesetzlicher Vorschriften zu kooperieren. Auf Verlangen des Kunden und auf dessen Kosten wird Infor im Falle eines Informationssicherheitsvorfalls (soweit gesetzlich und unter Wahrung angemessener Vertraulichkeit zulässig) dem Kunden Kopien der Aufzeichnungen über die betreffenden Systemaktivitäten (ausschließlich in Bezug auf den Informationssicherheitsvorfall, soweit er den Kunden betrifft) zur Verwendung in einem rechtlichen oder behördlichen Verfahren des Kunden oder in einer behördlichen Untersuchung des Kunden zur Verfügung stellen.

8. Protokollierung und Überwachung

Infor überwacht seine Ressourcen, die für die Bereitstellung der Services eingesetzt werden, mit einer Reihe von Tools, die speziell für die Verwaltung von Protokollen und Warnungen konfiguriert sind. Die Protokollaufzeichnungen werden physisch und virtuell gesichert, um Manipulationen zu verhindern. Sensible Informationen und Passwörter werden unter keinen Umständen protokolliert. Zusätzlich zur Erfassung von Informationen in Bezug auf die Services ermöglichen die Überwachungstools den Administratoren, die Nutzeraktivitäten beim Zugang und Verlassen des Systems nachzuverfolgen.

9. Sicherheit in Bezug auf Infor Mitarbeiter und Schulung

Infor-Mitarbeiter, die in die Bereitstellung der Services eingebunden sind, unterliegen Vertraulichkeitsverpflichtungen, kennen sich mit Bedrohungen und Problemen der Informationssicherheit aus, erhalten mindestens einmal im Jahr eine allgemeine Sicherheitsschulung und sind in der Lage, die Informationssicherheitsrichtlinien des Unternehmens sowohl allgemein als auch im Rahmen ihrer spezifischen Arbeitsaufgaben zu unterstützen.

10. Endgerätesteuerung (Infor Laptop, Workstations und mobile Geräte)

Infor implementiert allgemein anerkannte, branchenübliche Sicherheitsmaßnahmen zum Schutz der Endgeräte, einschließlich der Automatisierung des Patch-Managements für Anwendungen und Betriebssysteme sowie des Virenschutzes.

11. Rückgabe und Vernichtung von DATEN

11.1. Rückgabe

Bei Beendigung oder Ablauf der Cloud Services stellt Infor dem Kunden unverzüglich (innerhalb von 3-5 Werktagen nach Erhalt der schriftlichen Anfrage des Kunden im Wege eines Support Tickets) alle Kundendaten als nativen Datenbankexport über Infors sicheren Datenübermittlungsdienst (File Transfer Service) zur Verfügung. Wünscht der Kunde die Rückgabe der Kundendaten in einem anderen Format oder andere Unterstützungsleistungen bei der Beendigung, vereinbaren Infor und der Kunde den Umfang dieser Unterstützungsleistungen sowie die für diese Unterstützungsleistungen zu zahlenden Gebühren und Aufwendungen. Vor einer Beendigung hat der Kunde über die Schnittstellen der Applikation Zugriff auf die Kundendaten. Des Weiteren wird Infor vor einer Beendigung, auf Anfrage des Kunden über das Support Portal, bis zu zwei Mal innerhalb eines 12-Monatszeitraums eine Kopie des Data Backups als nativen Datenbankexport über Infors sicheren Datenübermittlungsdienst (File Transfer Service) zur Verfügung stellen. Für die Bereitstellung weiterer Kopien fällt eine Gebühr an.

Sofern nicht in vorliegendem Abschnitt 11 abweichend geregelt oder sofern nicht anderweitig von Infor für die Erbringung der Services benötigt, wird Infor auf Anfrage des Kunden, diesem die Kundendaten zurückgeben. Des Weiteren wird klargestellt, dass eine Rückgabe oder Vernichtung Personenbezogener Daten im Einklang mit den Regelungen der Datenschutzvereinbarung erfolgt.

11.2. Vernichtung der Daten

Mit Ausnahme im Rahmen einer vom Kunden in angesprochenen Transition Assistance, wird Infor alle (online oder über das Netzwerk zugänglichen) Instanzen von Kundendaten innerhalb von 35 Tagen nach der Beendigung der Cloud Services im Einklang mit NIST 800-88 dauerhaft löschen.

DATEN, die Infor für die Erbringung von Support zur Verfügung gestellt werden (d.h. durch ein im Supportportal geloggtes Support Ticket), werden fünf Jahre nach Schließung des Support-Tickets gelöscht. Individuelle Namen und Kontaktdaten des Kunden (z.B. die E-Mail-Adresse, der Name und die Telefonnummer eines Nutzers), die für das Bearbeitung und Administration des Support Ticket verwendet werden, werden bei Beendigung des Supports deaktiviert und auf Anfrage des Kunden, gelöscht.

12. Subunternehmer

Subunternehmer von Infor, die Infor Waren und Dienstleistungen in Bezug auf die Services von Infor liefern, müssen diese Waren und Dienstleistungen zu Bedingungen liefern, die im Wesentlichen denen dieses ISP entsprechen. Vor der Beauftragung eines solchen Subunternehmers mit der Erbringung der Services im Rahmen

dieses ISP prüft Infor dieses Unternehmen mit angemessener Sorgfalt, um sicherzustellen, dass das Unternehmen die Vertraulichkeits- und Sicherheitsverpflichtungen im Rahmen dieses ISP einhalten kann. Infor ist für alle Handlungen seiner Subunternehmer im Rahmen der Unterstützung der Services verantwortlich.