



Informationssicherheitsplan BPCS/LX, XA, System 21

Dieser Informationssicherheitsplan ("ISP") ist Bestandteil des Bestellformulars zwischen Infor und dem Kunden und legt die aktuellen Sicherheitsmaßnahmen von Infor dar, die dazu bestimmt sind, die Hardware, Geräte und Systemsoftwarekonfiguration zu schützen, (i) auf der Infor die Nutzung der Abonnierten-Software (wie im Bestellformular dargelegt) und die zugehörigen Abonnierten Dienstleistungen unterstützt, und (ii) auf der Kundendaten zur Nutzung durch oder mit der Abonnierten Software durch den Kunden oder seine Autorisierten User bereitgestellt, eingegeben oder hochgeladen wurden ((i) und (ii) zusammen die "Systeme"). Zur Klarstellung haben die in diesem ISP verwendeten und nicht definierten Begriffe in Großbuchstaben die Bedeutung, die diesen Begriffen in dem Software as a Service Vertrag zwischen Infor und dem Kunden (der "Vertrag") gegeben wird. Dieser ISP gilt nicht für Managed Service-Verträge von Infor, bei denen die Software des Kunden vor Ort von Infor gemäß einer separat ausgehandelten Vereinbarung über professionelle Dienstleistungen gehostet wird.

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 Kundendaten aufrechterhält.

1. Allgemeine Sicherheitsstandards

Infor unterhält administrative, technische und physische Sicherheitsvorkehrungen zum Schutz vor Zerstörung, Verlust, unbefugtem Zugriff oder Veränderung der Systeme und der Kundendaten, die Infor auf Anweisung des Kunden verarbeitet, (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 Kundendaten erhält, einschließlich der folgenden Maßnahmen:

- i. Infor weist jeder Person mit Computerzugang zu Kundendaten eine eindeutige ID zu.
- ii. Infor bestimmt die Mitarbeiter, die den Zugriff auf Kundendaten gewähren, ändern oder aufheben dürfen, und beschränkt den Zugriff auf Kundendaten auf der Basis des Prinzips der geringsten Berechtigung (least-privilege basis). Der Zugriff auf Kundendaten ist nur Mitarbeitern gestattet, die für die Bereitstellung von Abonnierten Dienstleistungen „Kenntnis haben müssen“, und Infor führt und aktualisiert eine Liste dieser Mitarbeiter. Ein solcher Zugriff wird protokolliert und überwacht.
- iii. Infor weist seine Mitarbeiter, die Zugriff auf Kundendaten haben, an, administrative Sitzungen zu beenden, wenn die Computer unbeaufsichtigt sind.

- iv. Infor deaktiviert die Konten von Infor-Mitarbeitern bei Anwendungen oder Datenspeichern, die Kundendaten enthalten, wenn diese Mitarbeiter entlassen oder versetzt werden oder wenn sie keinen Zugriff mehr auf diese Kundendaten benötigen. Infor überprüft regelmäßig die Liste der Personen und Dienste, die Zugriff auf Kundendaten haben, und entfernt Konten, die diesen Zugriff nicht mehr benötigen. Infor führt diese Überprüfung mindestens halbjährlich durch.
- v. Infor verwendet auf allen Systemen keine vom Hersteller vorgegebenen Standardwerte für Passwörter und andere Sicherheitsparameter. Infor schreibt die Verwendung von systemerzwungenen „starken Passwörtern“ vor, die den allgemein anerkannten Best Practices der Branche auf allen Infor-Systemen entsprechen. Infor verlangt, dass alle Passwörter und Zugangsdaten vertraulich behandelt und nicht an andere Mitarbeiter weitergegeben werden, und Infor deaktiviert Passwörter, von denen bekannt ist, dass sie beschädigt oder offengelegt wurden.
- vi. Infor hält eine „Kontosperre“ aufrecht, indem Konten mit Zugang zu Kundendaten gesperrt werden, wenn ein Konto mehr als eine definierte Zahl an aufeinanderfolgenden falschen Passworteingaben aufweist.
- vii. Der Fernzugriff auf Systeme mit Kundendaten 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 Einbruchversuche) und verdächtige interne Aktivitäten (z.B. nicht autorisierter Zugriff durch Systemadministratoren, nicht autorisierte Änderungen an den Systemen, Systemmissbrauch oder -diebstahl oder falsche Handhabung von Kundendaten). Infor überprüft die Zugriffsprotokolle regelmäßig auf Anzeichen von böartigem Verhalten oder unbefugtem Zugriff.

1.4. Firewall

Infor unterhält eine Netzwerk-Firewall-Technologie zum Schutz von Konnektivität und gehostete Umgebungen, die über das Internet zugänglich sind.

1.5. Aktualisierungen

Infor hält die abonnierten Systeme mit Upgrades, Updates, Fehlerbehebungen und neuen Versionen auf dem neuesten Stand. Updates/ Upgrades/ Korrekturen für Betriebssysteme und Anwendungssysteme werden mit dem Kunden abgestimmt, u.a. auch zeitlich.

1.6. Datenverschlüsselung

- i. Bei der Übertragung über öffentliche Netze werden die Kundendaten mindestens mit TLS 1.2 oder dessen logischem Nachfolger verschlüsselt.
- ii. Während sich die Kundendaten in den Systemen befinden, werden sie mindestens mit AES 256 Bit oder einem logischen Nachfolger verschlüsselt.

1.7. Identitätsmanagement

Infor wendet ein geteiltes Sicherheitskonzept an. Infor ist in der Lage, die Anwendungen in den Systemen

1.9. 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

Infor stellt Antworten auf den Fragebogen der Cloud Security Alliance (CSA) Consensus Assessments Initiative (CAIQ) zur Verfügung, der jährlich aktualisiert wird.

Im Rahmen seines Programms zur Überwachung von Dienstleistern können der Kunde und (falls zutreffend) seine staatliche Aufsichtsbehörde einmal pro Jahr in Form eines Post-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, dass Infor, soweit eine solche Verfahrensdokumentation ohne wesentlichen Aufwand verfügbar ist, dem Kunden eine solche Dokumentation in angemessenem Umfang zur Verfügung stellt, 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 Abonnierte Dienstleistungen 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 eine Vereinbarung zur Beantwortung treffen. Alle diese Unterlagen sind Vertrauliche Informationen von Infor. Infor wird die Erkenntnisse des Kunden, die sich aus diesem Post-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 Abonnierten Dienstleistungen durchzuführen. Der Prüfer wird von Infor beauftragt, einen Bericht in Übereinstimmung mit dem American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18) oder einem gleichwertigen Standard, der ISAE 3402 einschließen kann, zu erstellen (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.

Darüber hinaus wird Infor einmal pro rollierenden Zwölfmonatszeitraum während der Laufzeit des Abonnements auf eigene Kosten einen ordnungsgemäß qualifizierten unabhängigen Prüfer beauftragen, nach ISO 27001 eine Überprüfung der Informationssicherheit in Verbindung mit den Abonnierten Dienstleistungen für bestimmte auf trust.infor.com aufgeführte mandantenfähige (Multi-Tenant) Abonnierte Software durchzuführen. Der Prüfer wird von Infor beauftragt, einen Bericht in Übereinstimmung mit dem Standard der International Organization for Standardization (ISO) 27001 zu erstellen. Dieser Prüfbericht wird dem Kunden nicht zur Verfügung gestellt. Der Kunde kann jedoch jederzeit eine Kopie des daraus resultierenden Zertifikats von Infor's Cloud-Security-Seite (trust.infor.com) beziehen. Die Abonnierte Software, die Gegenstand des

Prüfberichts ist, wird in dem Zertifikat namentlich aufgeführt. Als Teil dieser ISO 27001-Zertifizierung unterhält Infor ein Informationssicherheits-Managementsystem-Handbuch für die von der Zertifizierung erfassten Abonnierten Software und den diesbezüglichen Abonnierten Dienstleistungen, welches dazu beiträgt, den Schutz, die Vertraulichkeit, die Integrität und die Verfügbarkeit der Infor-Ressourcen zu gewährleisten, die zur Bereitstellung solcher Abonnierten Dienstleistungen eingesetzt werden.

3. Änderungsmanagement

Infor folgt einem Änderungskontrollprozess, der die Identifizierung und Implementierung von Änderungen innerhalb der Ressourcen für die Abonnierten Dienstleistungen 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 Abonnierten Dienstleistungen 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 Kundendaten; keine Verwertung

4.1. Trennung

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

Infor kann 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 und den Betrieb der Abonnierten Software und Abonnierten Dienstleistungen durch den Kunden generiert werden.

5. Asset-Management

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

- i. Führung eines Inventars der für die Erbringung von Abonnierten Dienstleistungen verwendeten Anlagen und Einrichtungen ("Assets"), Festlegung eindeutiger Eigentumsverhältnisse und Kontrolle über die Assets, Fähigkeit zur Identifizierung der Assets und Verwaltung der Rückgabe, Vernichtung oder Entfernung von Kundendaten aus den betreffenden Assets; und
- ii. Verfahren zum Schutz von Assets vor internen oder externen, vorsätzlichen oder zufälligen Bedrohungen und Schwachstellen.

6. Scanning von Schwachstellen (Vulnerability 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

Zeitraumen. 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, einschließlich manueller Tests, um die Sicherheitskontrollen von Mehrmandantensystemen (Multi-Tenant) nach allgemein anerkannten Industriestandardmethoden zu bewerten.

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

7. Reaktion auf Informationssicherheitsvorfälle

Wenn Infor Kenntnis davon erlangt, dass Kundendaten auf eine nicht durch diesen ISP autorisierten Weise genutzt oder offengelegt werden oder eine solche Nutzung oder Offenlegung nach vernünftigen Maßstäben zu erwarten ist (ein "Informationssicherheitsvorfall"), wird Infor (i) den 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 zulässig und unter Wahrung angemessener Vertraulichkeit) 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 von Abonnierten Dienstleistungen 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 Dienstleistungen ermöglichen die Überwachungstools den Administratoren, die Benutzeraktivitäten beim Zugang und Verlassen des Systems nachzuverfolgen.

9. Sicherheit in Bezug auf Infor Mitarbeiter

Infor-Mitarbeiter, die in die Bereitstellung der Abonnierten Dienstleistungen 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 Kündigung oder Ablauf der Abonnierten Dienstleistungen stellt Infor dem Kunden unverzüglich (innerhalb von 3-5 Werktagen nach Erhalt der schriftlichen Anfrage des Kunden) alle Kundendaten als nativen Datenbankexport über den FTP-Server von Infor 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.

11.2. Vernichtung der Daten

Infor wird alle (online oder über das Netzwerk zugänglichen) Instanzen von Kundendaten innerhalb von 30 Tagen nach der Beendigung der Abonnierten Dienstleistungen dauerhaft löschen. Infor wird allgemein anerkannte, branchenübliche Verfahren zur Entsorgung von Hardware und physischen Komponenten mit Kundendaten anwenden. Alle Speichermedien werden elektronisch gelöscht (zeroed), bevor sie in der Infor-Produktivumgebung eingesetzt oder außer Betrieb genommen werden.

12. Subunternehmer

Subunternehmer von Infor, die Infor Waren und Dienstleistungen in Bezug auf die Abonnierten Dienstleistungen 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 von Abonnierten Dienstleistungen 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 Abonnierten Dienstleistungen verantwortlich.