Plan Bezpieczeństwa Informacji

Okres: Niniejszy Plan Bezpieczeństwa Informacji (dalej: „**ISP**”) stanowi część Formularza Zamówienia składanego Infor przez Klienta w nim oznaczonego i określa podejmowane przez Infor bieżące środki bezpieczeństwa mające na celu zabezpieczenie urządzeń:

i. sprzętu i konfiguracji oprogramowania systemów,a. wykorzystywanych przez Infor do wspierania:
   a. Usług w chmurze (dla jasności Usługi w chmurze obejmują W)sparcie,
   b. Usług Profesjonalnych a także
   c. Wsparcie dotyczące Oprogramowania typu On-Premise

(jakelkowiek sprzęt i konfiguracja oprogramowania systemowego są zdefiniowane
w niniejszym ISP jako "Systemy", a Usługi w chmurze, Usługi Profesjonalne i Wsparcie oprogramowania typu On-Premise są łącznie zdefiniowane w niniejszym ISP jako "Usługi"); jak również

Ii Dane Klienta przekazane Infor:
   a. jako dane Klienta, lub
   b. dostarczone Infor w celu świadczenia Usług Profesjonalnych i/lub Wspacia z poziomu środowiska Infor

   (wszystkie takie dane są zbiorczo zdefiniowane w niniejszym ISP jako „Dane”).

Definicje: Zaczynające się wielką literą terminy użyte w tym ISP i nie zdefiniowane w tym ISP mają znaczenie określone w Umowie na Oprogramowanie między Infor i Klientem („Umowa”).

Wyłączenia: Niniejszy ISP nie ma zastosowania do : (i) Usług Profesjonalnych Infor, gdzie Oprogramowanie typu On-Premise Klienta jest hostowane przez Infor zgodnie z osobno negocjowaną umową Usług Profesjonalnych, lub (ii) gdy Infor świadczy usługi w siedzibie Klienta i/lub ma dostęp do systemów Klienta. W takich przypadkach Infor będzie przestrzegać administracyjnych, technicznych i fizycznych warunków Klienta, ustalonych wzajemnie w oświadczeniu o pracy, i w związku z takim dostępem do systemów Klienta, Klient będzie odpowiedzialny za udzielenie personelowi Infor uprawnień użytkownika oraz haseł dostępu do systemów i odwoływanie takich uprawnień i kończenie takiego dostępu, zgodnie z własną oceną Klienta.

Aktualizacje: Zagrożenia bezpieczeństwa jak i środki mające na celu ochronę przed takimi zagrożeniami, stale ewoluują, w związku z czym Infor może w dowolnym momencie zmienić niniejszy ISP nie powiadamiając Klienta o tym fakcie, pod warunkiem, że Infor utrzyma porównywalny lub wyższy ogólny poziom bezpieczeństwa Systemów i Danych Klienta.

1. Ogólne Standardy Bezpieczeństwa

Infor utrzymuje administracyjne, techniczne i fizyczne zabezpieczenia mające na celu ochronę Systemów, oraz Danych Klienta przetwarzanych przez Infor na polecenie Klienta, przed zniszczeniem, utratą, nieuprawnionym dostępem lub zmianą, które to zabezpieczenia są: (i) nie mniej rygorystyczne niż te utrzymywane przez Infor dla jego własnych informacji o podobnym charakterze; (ii) nie mniej rygorystyczne niż powszechnie przyjęte standardy branżowe; oraz (iii) wymagane przepisami obowiązującego prawa.

1.1 Specjalista ds. Bezpieczeństwa

Infor wyznaczył jednego (lub kilku) specjalistę ds. bezpieczeństwa, odpowiedzialnego za koordynowanie i monitorowanie środków bezpieczeństwa przewidzianych w niniejszym ISP.

1.2 Kontrola Dostępu

Infor wdraża środki kontroli dostępu do Danych Klienta, w tym następujące:

i. Infor nadaje niepowtarzalny identyfikator każdej osobie mającej za pośrednictwem komputera dostęp do Danych Klienta.

ii. Infor identyfikuje personel uprawniony do udzielania, zmieniania lub odwoływania dostępu do Danych Klienta oraz ogranicza dostęp do Danych Klienta na zasadzie najmniejszego uprzywilejowania. Dostęp do Danych Klienta dozwolony jest wyłącznie dla personelu, któremu jest on niezbędny (na zasadzie ograniczonego dostępu) do świadczenia Subskrybowanych Usług, przy czym Infor prowadzi i aktualizuje rejestr takiego personelu. Dostęp jest w tym przypadku rejestrowany i monitorowany.

iii. Infor instruuje swój personel mający dostęp do Danych Klienta, aby kończył sesje administracyjne jeśli komputery są pozostawione bez nadzoru.

iv. Infor dezaktywuje konta swoich pracowników w ramach aplikacji lub repozytoriów danych zawierających Dane Klienta z chwilą rozwiązania z nimi stosunku pracy lub ich przeniesienia, lub z chwilą, gdy ustaje konieczność uzyskiwania przez nich dostępu do Danych Klienta. Infor okresowo aktualizuje listę osób i usług mających dostęp do Danych Klienta i usuwa konta, które nie wymagają już takiego dostępu. Infor dokonuje takiej aktualizacji co najmniej dwa razy w roku.

v. Infor nie wykorzystuje, w ramach żadnych Systemów, ustalonych przez producenta domyślnych haseł i innych parametrów bezpieczeństwa. Infor zezwala, we wszystkich Systemach Infor, na wykorzystanie narzucanych przez system „silnych haseł", zgodnie z powszechnie przyjętymi najlepszymi praktykami branżowymi. Infor wymaga zachowania w poufności wszystkich haseł i danych dostępowych oraz nieujawniania ich innym członkom personelu, przy czym Infor dezaktywuje hasła, co do których wiadomo, że zostały uszkodzone lub ujawnione.

vi. Infor dysponuje mechanizmem „blokady konta" poprzez wyłączenie konta z dostępem do Danych Klienta po określonej liczbie następujących kolejno po sobie prób wprowadzenia nieprawidłowego hasła.

vii. Zdalny dostęp do Systemów zawierających Dane Klienta wymaga dwustopniowego uwierzytelnienia (np. wymaga co najmniej dwóch odrębnych stopni identyfikacji użytkowników).

1.3 **Włamania - Wykrywanie i Zapobieganie**

Infor wykorzystuje system wykrywania włamań (IDS)/system zapobiegania włamaniom (IPS) w celu monitorowania swoich Systemów i procedur w zakresie naruszeń bezpieczeństwa i podejrzanej aktywności. Obejmuje on zarówno kontrolę podejrzanej aktywności zewnętrznej (w tym między innymi prób nieuprawnionego sondowania, skanowania lub włamania), jak i podejrzanej aktywności wewnętrznej (w tym między innymi nieuprawnionego dostępu do administracji systemu, nieautoryzowanych zmian Systemów, nieprawidłowego korzystania z Systemów lub ich kradzież, oraz nieprawidłowego postępowania z Danymi Klienta). Infor okresowo przegląda dzienniki kontroli dostępu w poszukiwaniu oznak złośliwego zachowania lub nieuprawnionego dostępu.

1.4 **Zapora Sieciowa (ang. Firewall)**

Infor utrzymuje technologię zapory sieciowej mającej na celu ochronę Danych Klienta dostępnych z poziomu sieci Internet.

1.5 **Aktualizacje**

Infor na bieżąco aktualizuje Systemy poprzez wprowadzanie ulepszeń, aktualizacji, a także odpluskwianie i wydawanie nowych wersji.

1.6 **Szyfrowanie Danych**

- W trakcie przesyłania za pośrednictwem sieci publicznych Dane Klienta są szyfrowane za pomocą, co najmniej, protokołu TLS 1.2 lub jego logicznego następcy.

- Gdy Dane Klienta znajdują się w stanie spoczynku w zasobach Systemów są one szyfrowane za pomocą, co najmniej, protokołu 256-bitowego protokołu AES lub jego logicznego następcy.

1.7 **Zarządzanie Tożsamościami**

Infor doskonali model podziału bezpieczeństwa w celu rozproszenia kwestii bezpieczeństwa. Infor ma możliwość stowarzyszania aplikacji w ramach Systemów z dostawcą tożsamości po stronie Klienta.

1.8 **Złośliwe Oprogramowanie**

Infor utrzymuje powszechnie przyjęty branżowy standard w zakresie oprogramowania przeciw złośliwemu oprogramowaniu i oprogramowania antywirusowego oraz, w miarę możliwości, wykorzystuje funkcje ochrony w czasie zbliżonym do rzeczywistego w ramach starań, aby Usługi w chmurze nie zawierały „bomb czasowych", „robaków komputerowych", „wirusów", „koni trojańskich", „kodów ochronnych", „kluczy niszczących dane" oraz innych metod programowania mających na celu (i) w odniesieniu do Usług w chmurze, modyfikować, usuwać, uszkadzać, dezaktywować lub wyłączać Dane Klienta lub uniemożliwiać lub ograniczać dostęp Klienta do Danych Klienta lub (ii) w odniesieniu do Oprogramowania typu On-Premise, modyfikować, usuwać, uszkadzać, dezaktywować lub wyłączać dane Klienta w ramach Oprogramowania typu On-Premise..

1.9 **Bezpieczeństwo Fizyczne.**

Obiekty, w których znajdują się Systemy:

(a) zostaną zaprojektowane tak, aby wytrzymać niekorzystne warunki pogodowe i inne zasadnie dające się przewidzieć warunki atmosferyczne;

(b) zostaną zaopatrzone w stosowne fizyczne zabezpieczenia środowiskowe w celu ochrony systemów przed uszkodzeniem spowodowanym dymem, wysokimi temperaturami, wodą, ogniem, wilgotnością i wahaniami zasilania;

(c) będą wspierane przez lokalne systemy zasilania zapasowego; oraz

(d) zostaną wyposażone w odpowiednie środki kontrolne zaprojektowane tak, aby zapewnić, że fizyczny dostęp do obiektu będzie mieć wyłącznie uprawniony personel.

2. **Audyt**

2.1 **Prawa w zakresie Audytu**

W ramach programu nadzoru nad dostawcami Klient, oraz (jeśli dotyczy) organ regulacyjny, może zażądać, raz do roku w formie audytu korespondencyjnego (tj. kwestionariusza zgodnego z normą ISO 27001), przedstawienia przez Infor dokumentacji proceduralnej dotyczącej obowiązującego programu, procesów i kontroli bezpieczeństwa informacji. Infor wyraża zgodę, że w miarę dostępności takiej dokumentacji proceduralnej przedstawi on taką dokumentację, jakiej Klient zasadnie zażąda pod warunkiem, że (a) nie zagraża ona poufności, integralności lub dostępności danych lub usług innych klientów Infor lub (b) nie narusza ona poufności, integralności lub dostępności danych lub usług stron trzecich świadczących Subskrybowane Usługi na rzecz klienta w imieniu Infor. Dokumentacja proceduralna przedstawiona przez Infor nie będzie zawierać materiału dowodowego (przykładowo, między innymi, dowodów odbycia szkoleń, dowodów przeprowadzenia testów, wyników ocen ryzyka). Infor odpowie na kwestionariusz w ciągu trzydziestu (30) dni; zaś w razie niemożności dochowania tego terminu, Infor będzie współpracować z Klientem w celu uzgodnienia terminu jego wypełnienia. Wszelką taką dokumentację poczytuje się jako Informacje Poufne Infor. Infor nie weźmie pod uwagę ustaleń Klienta wynikających z takiego audytu korespondencyjnego.

2.2 **Audyt Zewnętrzny**

Raz w ciągu każdego 12-miesięcznego okresu w trakcie Okresu Subskrypcji Infor, na własny koszt, zatrudni należycie wykwalifikowanego niezależnego audytora do przeprowadzenia kontroli projektu i wydajności operacyjnej zdefiniowanych przez Infor celów i czynności kontrolnych w związku z Usługami w chmurze (z wyjątkiem Wsparcia). Infor sprawi, że taki audytor sporządzi sprawozdanie raportu SOC I Typ 2 dla wszystkich Usług w chmurze oraz, wyłącznie dla Usług w chmurze dla multi-tenant, raportu SOC II Typ 2 (zwanych łącznie "Raportem z Audytu"). Klient może udostępnić kopię takiego Raportu z Audytu swoim audytorom i organom regulacyjnym, pod warunkiem, że audytorzy i organy regulacyjne zostaną poinformowani, że taki Raport z Audytu stanowi Informacje Poufne Infor i musi być odpowiednio chroniony.

Dodatkowo, raz w ciągu każdego 12-miesięcznego okresu w trakcie Okresu Subskrypcji Infor, na własny koszt, zatrudni należycie wykwalifikowanego niezależnego audytora do przeprowadzenia kontroli bezpieczeństwa informacji w związku z Usługami w chmurze dla niektórych Usług w chmurze w modelu *multi-tenant* wymienionych w trust.infor.com zgodnie z normą ISO 27001. Infor sprawi, że taki audytor sporządzi sprawozdanie zgodne z normą International

Organization for Standardization (ISO) 27001. Sprawozdanie z audytu nie zostanie przekazane Klientowi, aczkolwiek Klient może w dowolnej chwili uzyskać egzemplarz wydanego w związku z audytem certyfikatu dostępnego na stronie Infor poświęconej bezpieczeństwu usług w chmurze (trust.infor.com). W treści certyfikatu wskazane zostanie Subskrybowane Oprogramowanie, którego sprawozdanie dotyczy. W ramach wspomnianej certyfikacji ISO 27001 Infor dysponuje podręcznikiem dotyczącym Systemu Zarządzania Bezpieczeństwem Informacji dla Subskrybowanego Oprogramowania objętego certyfikatem oraz dla związanych z nim Subskrybowanych Usług w celu zapewnienia ochrony, poufności, integralności i dostępności zasobów Infor wykorzystywanych do świadczenia takich Usług.

Dodatkowe certyfikaty stron trzecich są udostępnione na trust.infor.com.

3. Dodatkowe certyfikaty stron trzecich są dostępne na trust.infor.com.Zarządzanie Zmianą dla Usług w chmurze

Infor przestrzega procesów kontroli zmiany, którym podlega identyfikacja i wdrażanie zmian w ramach zasobów Infor wykorzystywanych do świadczenia Usług w chmurze w celu zapobieżenia niechcianym zmianom kodu źródłowego aplikacji, interfejsów, systemów operacyjnych lub zmianom zaplecza technicznego danych w ramach istniejących obszarów i tabel. Wszelkie żądane zmiany zasobów Infor wykorzystywanych do świadczenia Usług w chmurze muszą być zgodne z procesem kontroli wdrażania zmiany. Infor dokumentuje i przechowuje szczegółową dokumentację w zakresie zgodności z tym procesem, przykładowo system nadawania numerów podejmowanych czynności, a także dokumentację procedur testowych dla dowolnej zmiany, w tym między innymi terminy i godziny wprowadzania takich zmian oraz opisy ich charakteru.

4. Segregacja Danych Klienta; Brak Eksploatacji

4.1 Segregacja

Dane Klienta przechowywane są w sposób logicznie odseparowany od danych Infor i od danych innych klientów Infor poprzez zastosowanie odpowiednich środków technicznych.

4.2 Brak Eksploatacji; Statystyki Zbiorcze

Dane Klienta poczytuje się jako Informacje Poufne Klienta, zaś Klient pozostaje właścicielem wszelkich praw rzeczowych względem Danych Klienta. Infor nie będzie w sposób komercyjny eksploatować Danych Klienta i nie uzyska dostępu do Danych Klienta w innym zakresie niż wymaganym do świadczenia Usług oraz do wykonania zobowiązań wynikających z Umowy.

Infor może gromadzić Statystyki Zbiorcze, które pozostają wyłączną własnością Infor i których nie poczytuje się jako Dane Klienta. „Statystyki Zbiorcze" oznaczają dane statystyczne oraz informacje dotyczące wydajności, wygenerowane przez instrumenty i systemy rejestrujące, dotyczące korzystania przez Klienta z Usług oraz ich obsługi.

5. Zarządzanie Zasobami

W Infor obowiązuje formalny proces zarządzania zasobami, który obejmuje

- prowadzenie ewidencji zasobów wykorzystywanych do świadczenia Usług (dalej: „Zasoby"), ustalanie jasnej struktury własności Zasobów i kontroli nad nimi, możliwość identyfikacji Zasobów,
- zarządzanie zwrotami, niszczeniem i usuwaniem Danych Klienta z odnośnych Zasobów; oraz
- procedury zaprojektowane w celu ochrony Zasobów przed zagrożeniami i podatnością na nie, zarówno wewnętrznymi, jak i zewnętrznymi, zamierzonymi i nieumyślnymi.

6. Skanowanie pod kątem podatności na zagrożenia i testy penetracyjne

W Infor obowiązują procesy zarządzania podatnością na zagrożenia polegające na skanowaniu pod kątem ryzyka wynikającego z eksploatacji opublikowanych lub zidentyfikowanych wad lub słabych punktów, które mogą być wykorzystane (nieumyślnie lub celowo) i mogą skutkować uszkodzeniem Systemów lub nieuprawnionym dostępem do nich (dalej: „**Podatność na Zagrożenia**"). Infor zajmie się Podatnościami na Zagrożenia w powszechnie przyjętych w branży standardowych terminach. Infor zaradzi skutkom zaistnienia Podatności na Zagrożenia, lub je zniweluje, w sposób współmierny do ryzyka, jakie takie Podatności na Zagrożenia ze sobą niosą, w zdefiniowanych przez Infor ramach zgodnych z powszechnie przyjętymi standardami branżowymi.

Infor co roku, na własny koszt, zleci stronie trzeciej wykonanie testów penetracyjnych według powszechnie przyjętych w branży standardowych metodologii, w tym obejmujących przeprowadzane przez człowieka testy ręczne, w celu oceny środków kontroli w ramach systemów współdzielonych w modelu *multi-tenant* bezpieczeństwa Systemów zgodnie z powszechnie przyjętymi standardowymi metodologiami branżowymi.

Dla Subskrybowanego Oprogramowania w modelu *multi-tenant* oceny w ramach testów bezpieczeństwa, w tym skanowanie kodów źródłowych i skanowanie pod kątem Podatności na Zagrożenia, przeprowadzane są przed wydaniem kodu i podczas całego cyklu życia produktu stanowiącego Uslugi w chmurze (tj. w środowiskach deweloperskich i produkcyjnych) w celu zidentyfikowania potencjalnych Podatności na Zagrożenia, którym należy zaradzić lub które należy zniwelować. Testy penetracyjne wykonywane są co roku w Systemach w modelu *multi-tenant* w celu zidentyfikowania Podatności na Zagrożenia, którym należy zaradzić lub które należy zniwelować.

7. Reakcja na Incydenty Naruszenia Bezpieczeństwa Informacji

W razie powzięcia przez Infor informacji o tym, że Dane zostały wykorzystane lub ujawnione w sposób niezgodny z niniejszym ISP, lub że istnieje uzasadnione podejrzenie, że mogło do tego dojść (dalej: „Incydent Naruszenia Bezpieczeństwa Informacji"), wówczas Infor: (i) bezzwłocznie (zaś w każdym przypadku w ciągu 48 godzin od powzięcia informacji o takim Incydencie Naruszenia Bezpieczeństwa Informacji) powiadomi afektowanego Klienta o zaistnieniu takiego Incydentu Naruszenia Bezpieczeństwa Informacji; (ii) zbada i przeprowadzi zasadne analizy przyczyny (lub przyczyn) takiego Incydentu Naruszenia Bezpieczeństwa Informacji; (iii) będzie na bieżąco informować Klienta o przebiegu toczącego się badania; (iv) opracuje i wdroży odpowiedni plan zaradzenia przyczynie takiego Incydentu Naruszenia Bezpieczeństwa Informacji w zakresie, w jakim Infor ma na taką przyczynę wpływ; oraz (v) będzie współpracować z Klientem przy zasadnych prowadzonych przez Klienta badaniach lub dążeniach Klienta do spełnienia wszelkich wymogów informacyjnych i regulacyjnych mających zastosowanie do takiego Incydentu Naruszenia Bezpieczeństwa Informacji. Na żądanie Klienta, oraz na jego koszt, w razie zaistnienia Incydentu Naruszenia Bezpieczeństwa Informacji, Infor przedstawi Klientowi (w zakresie dozwolonym przepisami obowiązującego prawa i z zastrzeżeniem zachowania odpowiedniego poziomu poufności) egzemplarze dokumentacji aktywności odnośnych Systemów (wyłącznie w odniesieniu do Incydentu Naruszenia Bezpieczeństwa Informacji dotyczącego Klienta) do wykorzystania podczas wszelkich postępowań prawnych lub przed organami regulacyjnymi, których Klient jest stroną lub podczas wszelkich toczących się względem Klienta postępowań wyjaśniających prowadzonych przez organy państwowe.

8. Rejestracja i Monitorowanie

Infor monitoruje swoje zasoby wykorzystywane do świadczenia Subskrybowanych Usług wykorzystując zestaw narzędzi skonfigurowanych pod kątem zarządzania rejestrami i alertami. Wpisy w rejestrach są zabezpieczone fizycznie i wirtualnie w celu zapobieżenia manipulowaniu nimi. Informacje wrażliwe i hasła nigdy nie są rejestrowane. Oprócz przechwytywania informacji związanych z usługami, narzędzia monitorujące umożliwiają administratorom śledzenie aktywności użytkowników wchodzących do systemu i wychodzących z niego.

9. Bezpieczeństwo Zasobów Ludzkich

Personel Infor świadczący Subskrybowane Usługi podlega zobowiązaniom w zakresie poufności, jest zaznajomiony z rodzajami zagrożeń i obaw w związku z bezpieczeństwem informacji, co najmniej raz do roku przechodzi ogólne szkolenie w zakresie bezpieczeństwa, oraz dysponuje sprzętem umożliwiającym wspieranie obowiązujących w organizacji polityk bezpieczeństwa informacji, zarówno ogólnych, jak i związanych konkretnie z zajmowanymi stanowiskami.

10. Kontrola Urządzeń Końcowych (Laptopów, Stanowisk Pracy, Urządzeń Mobilnych Infor)

Infor wdraża powszechnie przyjęte branżowe praktyki w zakresie bezpieczeństwa w celu ochrony urządzeń końcowych, w tym automatyzację zarządzania łatkami oprogramowania dla aplikacji i systemów operacyjnych oraz ochronę antywirusową.

11. Zwrot Danych i ich Niszczenie

11.1. Zwrot

Z chwilą zakończenia świadczenia lub wygaśnięcia Usług w chmurze, Infor bezzwłocznie (w ciągu 3-5 dni roboczych od otrzymania od Klienta pisemnego żądania poprzez wysłanie standardowego zgłoszenia do Pomocy Technicznej) udostępni Klientowi wszystkie Dane Klienta w formie wyciągu z zasobów natywnej bazy danych za pośrednictwem usługi bezpiecznego przesyłania plików. Przed zakończeniem, Klient ma dostęp do danych klienta poprzez interfejsy

aplikacji i Klient może poprzez portal wsparcia poprosić o kopie danych z kopii zapasowej nie więcej niż dwa razy w ciągu 12 miesięcy; wszelkie dodatkowe żądania podlegają opłatom.

11.2. Zniszczenie

Z wyjątkiem przypadków, w których Klient zażądał Pomocy w Przejściu, Infor trwale usunie wszystkie (dostępne online lub w sieci) instancje Danych Klienta w ciągu 35 dni od zakończenia lub wygaśnięcia Usług w Chmurze zgodnie z NIST 800-88. Dane przekazane do Infor w celu świadczenia wsparcia (np. poprzez zgłoszenie wsparcia zarejestrowane w portalu Wsparcia) są usuwane po pięciu latach od daty zamknięcia zgłoszenia incydentu. Imię i dane kontaktowe klienta (np. adres e-mail, imię i numer telefonu użytkownika) używane do zarządzania cyklem życia zgłoszenia Wsparcia są dezaktywowane i zanonimizowane po zakończeniu Wsparcia.

Podwykonawcy

Podwykonawcy Infor realizujący dostawy towarów lub świadczący usługi na rzecz Infor w zakresie świadczonych przez Infor Usług czynią to na warunkach zbliżonych do tych, które są określone w niniejszym ISP. Przed zatrudnieniem zewnętrznego podwykonawcy do świadczenia dowolnych przewidzianych w niniejszym ISP Usług, Infor z należytą starannością zweryfikuje takiego zewnętrznego podwykonawcę w celu zapewnienia, że jest on w stanie wykonać przewidziane w niniejszym ISP zobowiązania w zakresie poufności i bezpieczeństwa. Infor odpowiada za wszystkie działania podejmowane przez swoich podwykonawców wspierających świadczenie Usług.

Wyłączenie odpowiedzialności: Do następujących produktów mogą mieć zastosowanie dodatkowe lub inne warunki w zakresie bezpieczeństwa: Anael (SaaS) (France); 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).