Plano de Segurança da Informação

Este Plano de Segurança da Informação (*Information Security Plan* o "ISP") é incorporado ao Formulário de Pedido entre a Infor e o Cliente nele nomeado e estabelece as medidas de segurança atuais da Infor destinadas a proteger a configuração de hardware, equipamento e configuração dos sistemas de software (i) nos quais a Infor suporta o uso do Software de Subscrição (estabelecido no Formulário de Pedido) e dos Serviços de Subscrição relacionados e, (ii) nos quais os Dados do Cliente foram fornecidos, inseridos ou carregados para uso por com o Software de Subscrição pelo Cliente ou seus Usuários Autorizados (i e ii coletivamente, os “Sistemas”). Para maior clareza, os termos em maiúsculas usados neste ISP, e não definidos aqui, têm o significado atribuído a tais termos no Contrato de Software Como Serviço entre a Infor e tal Cliente (o "Contrato"). Este ISP não se aplica aos acordos de Serviços gerenciados da Infor, nos quais a Infor hospeda o software on-premise do Cliente de acordo com um contrato de serviços profissionais negociado separadamente.

As ameaças de segurança e as medidas destinadas a proteger contra essas ameaças estão em constante evolução, portanto, a Infor pode alterar este ISP a qualquer momento sem aviso prévio ao Cliente, desde que a Infor mantenha um nível de segurança comparável ou melhor para o conjunto de Sistemas e Dados do Cliente.

1. Pautas Gerais de Segurança

A Infor mantém medidas proteções administrativas, técnicas e físicas destinadas a proteger contra destruição, perda, acesso ilegal ou alteração dos Sistemas e Dados do Cliente que a Infor processa sob a direção do Cliente, que são: (i) tão rigorosas do que as mantidas pela Infor por suas próprias informações de natureza semelhante; (ii) tão rigorosos quanto os padrões geralmente aceitos da indústria; e (iii) exigido pela lei aplicável.

1.1. Agentes de Segurança

A Infor designou um ou mais agentes de segurança responsáveis por coordenar e monitorar as medidas de segurança neste ISP.

1.2. Controles de Acesso

A Infor implementa controles de acesso aos Dados do Cliente, incluindo as seguintes medidas:

i. A Infor atribui uma identificação única a cada pessoa com acesso por computador aos Dados do Cliente.

ii. A Infor identifica o pessoal que pode conceder, modificar ou encerrar o acesso aos Dados do Cliente e restringe o acesso aos Dados do Cliente com base no privilégio mínimo. O acesso aos Dados do Cliente só é permitido ao pessoal que tenha "necessidade de saber" para fornecer os Serviços de Subscrição, e a Infor mantém e atualiza um registro desse pessoal. Esse acesso é registrado e monitorado.

iii. A Infor instrui seu pessoal que tem acesso aos Dados do Cliente a desativar as sessões administrativas quando os computadores não estiverem em uso.

iv. A Infor desativa as contas de seus funcionários de aplicativos ou armazéns de dados que contenham Dados do Cliente quando tais funcionários são demitidos ou transferidos, ou quando não precisam mais acessar esses Dados do Cliente. A Infor revisa periodicamente a lista de pessoas e serviços com acesso aos Dados do Cliente e exclui contas que não requerem mais tal acesso. A Infor realiza essa revisão pelo menos duas vezes por ano.

v. A Infor não usa senhas ou outras configurações de segurança padrão fornecidas por qualquer fabricante para qualquer Sistema. A Infor exige o uso de "senhas seguras" impostas pelo sistema em todos os Sistemas da Infor, de acordo com as melhores práticas geralmente aceitas do setor. A Infor exige ainda que todas as senhas e credenciais de acesso sejam mantidas em sigilo e não sejam compartilhadas entre os funcionários, além de desabilitar as senhas conhecidas por terem sido comprometidas ou divulgadas.

vi. A Infor mantém um "bloqueio de conta" desativando contas com acesso aos Dados do Cliente após superar um número especificado de tentativas consecutivas com senha incorreta.

vii. O acesso remoto a Sistemas que contêm Dados do Cliente requer autenticação de dois fatores (por exemplo, requer pelo menos dois fatores independentes para identificar usuários).

1.3. Detecção e Prevenção de Intrusão

A Infor utiliza um sistema de detecção de intrusão/sistema de prevenção de intrusão (IDS/IPS) para monitorar seus Sistemas e procedimentos quanto a brechas de segurança, violações e atividades suspeitas. Isso inclui atividades externas suspeitas (incluindo, mas não se limitando a, investigações não autorizadas, varreduras ou tentativas de intrusão) e atividades internas suspeitas (incluindo, mas não se limitando a, acesso não autorizado do administrador do sistema, alterações não autorizadas nos Sistemas, uso indevido ou roubo do Sistemas, ou manuseio incorreto de Dados do Cliente). A Infor revisa regularmente os logs de acesso em busca de sinais de comportamento malicioso ou acesso não autorizado.

1.4. Firewall

Infor mantém uma tecnologia de firewall de rede projetada para proteger os Dados do Cliente acessíveis através da Internet .

1.5. Atualizações

A Infor mantém os Sistemas atualizados com melhorias, atualizações, correções de bugs e novas versões.

1.6. Criptografia de Dados

i. No trânsito por redes públicas, os Dados do Cliente são criptografados com pelo menos TLS 1.2 ou seu sucessor lógico.

ii. Enquanto os Dados do Cliente estão em repouso nos Sistemas, os Dados do Cliente são criptografados com pelo menos AES de 256 bits ou seu sucessor lógico.

1.7. Gerenciamento de Identidade

A Infor aproveita um modelo de segurança compartilhado para distribuir segurança. A Infor tem a capacidade de federar os aplicativos nos Sistemas com o provedor de gerenciamento de identidade do Cliente.

1.8. Software Malicioso

A Infor mantém software antimalware/antivírus padrão geralmente aceito na indústria e, na medida do possível, usa recursos de proteção quase em tempo real em um esforço para fornecer Software de Subscrição e Serviços de Subscrição que não contenham "bombas-relógio", "worms", "vírus", "cavalos de Tróia", "códigos de proteção", "chaves de destruição de dados" ou outros dispositivos de programação destinado a acessar, modificar, eliminar, danificar, desativar ou desabilitar os Dados do Cliente ou para impedir ou limitar o acesso do Cliente aos Dados do Cliente (“Código Malicioso”). Após a descoberta, a Infor investigará, identificará e removerá tal Código Malicioso do Software de Subscrição e dos Serviços de Subscrição.

1.9. Segurança Física

As instalações que contêm os Sistemas:

i. serão estruturalmente desenhadas para resistir condições climáticas adversas e outras condições naturais razoavelmente previsíveis;

ii. terão medidas de proteção ambiental física apropriadas para ajudar a proteger os Sistemas contra danos relacionados a fumaça, calor, água, fogo, umidade ou flutuações na energia elétrica;

iii. serão suportadas por sistemas de geração de energia no sítio; e

iv. terão controles apropriados projetados para garantir que apenas pessoal autorizado tenha acesso físico às instalações.

2. Auditoria

2.1. Direitos de Auditoria

Como parte de seu programa de supervisão de fornecedores, o Cliente e (se aplicável) sua agência reguladora governamental, podem solicitar uma vez por ano na forma de uma auditoria postal (por exemplo, um questionário baseado na ISO 27001), documentação dos procedimentos da Infor com relação ao seu Plano de Segurança da Informação, processos e controles. A Infor concorda que, na medida em que tal documentação processual esteja prontamente disponível, a Infor fornecerá a documentação que o Cliente possa razoavelmente solicitar, desde que tal documentação não (a) ameace a confidencialidade, integridade ou disponibilidade dos dados ou serviços de outros Clientes de Infor, ou (b) viole a confidencialidade, integridade e disponibilidade de dados ou serviços de

terceiros que fornecem Serviços de Subscrição ao Cliente em nome da Infor. A documentação processual fornecida pela Infor não incluirá evidências (por exemplo, sem limitação, evidências de treinamento, evidências de testes, resultados de avaliações de risco). A Infor responderá ao questionário em até 30 dias; se este prazo não puder ser cumprido, a Infor trabalhará com o Cliente para concordar com a finalização do mesmo. Toda a documentação referida será Informação Confidencial da Infor. A Infor não considerará as descobertas do Cliente resultantes desta auditoria postal.

2.2. Auditoria de Terceiros

Uma vez em cada período de 12 meses durante o Período de Subscrição, a Infor deverá, às suas custas, contratar um auditor independente devidamente qualificado para realizar uma revisão do projeto e eficácia operacional dos objetivos e atividades de controle definidos pela Infor em conexão com os Serviços de Subscrição. A Infor solicitará ao referido auditor um relatório de acordo com o Declaração de Normas para Trabalhos de Certificação n.º 18 *(Statement on Standards for Attestation Engagements, SSAE 18)* do American Institute of Certified Public Accountants ou uma norma equivalente, que pode incluir o ISAE 3402 (o "Relatório de Auditoria"). O Relatório de Auditoria é informação confidencial da Infor, mas será disponibilizado ao Cliente no portal de suporte Infor. O Cliente pode compartilhar uma cópia de tal Relatório de Auditoria com seus auditores e reguladores, desde que os auditores e reguladores sejam informados de que tal Relatório de Auditoria é Informação Confidencial da Infor e deverá ser adequadamente protegido.

Além disso, uma vez a cada período de 12 meses durante o Período de Subscrição, a Infor manterá, às suas custas e despesas, um auditor independente devidamente qualificado para realizar uma análise de segurança da informação relacionada aos Serviços de Subscrição para determinado Software de Subscrição Multilocatário. declarado em www.trust.infor.com sob ISO27001. A Infor solicitará ao referido auditor um relatório de acordo com a norma 27001 da Organização Internacional para Padronização (*International Organization for Standardization)*. O relatório de auditoria não estará disponível para o Cliente; no entanto, o Cliente pode obter uma cópia do certificado resultante do site de segurança em nuvem da Infor (www.trust.infor.com) a qualquer momento. O certificado identificará o Software de Subscrição que corresponde ao relatório. Como parte desta certificação ISO 27001, a Infor mantém um manual do Sistema de Gerenciamento de Segurança da Informação para o Software de Subscrição incluído na certificação e os Serviços de Subscrição correspondentes, que ajuda a garantir a proteção, confidencialidade, integridade e disponibilidade dos ativos da Infor usados para fornecer tais Serviços de Subscrição.

3. Gerenciamento de Alterações

A Infor segue um processo de controle de alterações que rege a identificação e implementação de alterações nos recursos de entrega dos Serviços de Subscrição da Infor para ajudar a prevenir alterações indesejadas no código-fonte do aplicativo, interfaces, sistemas operacionais ou alterações no back-end em dados em campos e tabelas existentes. Quaisquer alterações solicitadas nos recursos de entrega dos Serviços de Subscrição da Infor devem seguir um processo de controle de alterações de implementação. A Infor documenta e mantém um registro detalhado de sua conformidade com este processo, como um sistema de tíquetes e registros de procedimentos de teste para quaisquer alterações, incluindo, sem limitação à data e hora de tal alteração e uma descrição da natureza da mesma.

4. Segregação de Dados do Cliente; Não Uso

4.1. Segregação

Os Dados do Cliente são mantidos logicamente separados dos dados da Infor e dos dados de qualquer outro cliente da Infor por meios técnicos apropriados.

4.2. Não Uso; Estatísticas Agregadas

Os Dados do Cliente constituem Informações Confidenciais do Cliente e o Cliente detém todos os direitos de propriedade sobre eles. A Infor não explorará comercialmente os Dados do Cliente e não acessará os Dados do Cliente, exceto conforme necessário para fornecer os Serviços de Subscrição e cumprir suas obrigações sob o Contrato.

Infor pode coletar estatísticas agregadas, que são de propriedade exclusiva da Infor e não são consideradas Dados do Cliente . "Estatísticas Agregadas" são dados estatísticos e informações de desempenho, gerados por meio de instrumentação e sistemas de registro, relacionados ao uso e operação do Software de Subscrição e dos Serviços de Subscrição pelo Cliente.

5. Gerenciamento de Ativos

A Infor possui um processo formal de gerenciamento de ativos que inclui:

i. Manter um inventário dos ativos usados para fornecer Serviços de Subscrição ("Ativos"), estabelecendo claramente a propriedade e o controle dos Ativos, sendo capaz de identificar os Ativos e providenciar a devolução, destruição ou remoção dos Dados do Cliente dos Ativos aplicáveis; e

ii. procedimentos destinados a proteger os Ativos de ameaças e vulnerabilidades, sejam internas ou externas, deliberadas ou acidentais.

6. Verificação de Vulnerabilidade e Teste de Penetração

A Infor mantém um processo de gerenciamento de vulnerabilidades para buscar riscos resultantes da exploração de falhas ou fraquezas publicadas ou identificadas que possam ser exercidas (acidentalmente ou intencionalmente) e resultar em danos ou acesso não autorizado aos Sistemas ("Vulnerabilidades"). A Infor tratará as Vulnerabilidades dentro dos prazos geralmente aceitos da indústria. A Infor irá corrigir ou mitigar as Vulnerabilidades de forma compatível com o risco representado por tais Vulnerabilidades, de acordo com a estrutura definida pela Infor, que é consistente com os padrões geralmente aceitos do setor.

Anualmente, a Infor contrata, às suas próprias custas, um terceiro independente para realizar testes de penetração, incluindo testes manuais humanos, para avaliar os controles de segurança de sistemas multilocatários seguindo metodologias padrão geralmente aceitas da indústria.

Para o Software de Subscrição multilocatário, as avaliações de teste de segurança, incluindo varreduras de código-fonte e varreduras de Vulnerabilidade, são realizadas antes do lançamento do código e durante todo o ciclo de vida do produto do Software de Subscrição (por exemplo, em ambientes de desenvolvimento e produção) para ajudar a identificar potenciais Vulnerabilidades que precisam ser corrigidas ou mitigadas. Anualmente, são realizados testes de penetração em Sistemas multilocatários para identificar Vulnerabilidades potenciais para seu reparo ou mitigação.

7. Resposta a Incidentes de Segurança da Informação

Se a Infor tomar conhecimento de que os Dados do Cliente foram, ou se espera que tenham sido, sujeitos a uso ou divulgação não autorizados por este ISP (um "Incidente de Segurança da Informação"), a Infor deverá: (i) notificar o Cliente sobre a ocorrência de tal Incidente de Segurança da Informação prontamente e sem atrasos indevidos (e em qualquer caso, dentro de 48 horas após tomar conhecimento de tal Incidente de Segurança da Informação); (ii) investigar e conduzir uma análise razoável da(s) causa(s) de tal Incidente de Segurança da Informação; (iii) fornecer atualizações periódicas sobre quaisquer investigação em andamento ao Cliente; (iv) desenvolver e implementar um plano apropriado para remediar a causa de tal Incidente de Segurança da Informação, na medida em que tal causa esteja sob o controle da Infor; e (v) cooperar com a investigação razoável do Cliente ou com os esforços do Cliente para cumprir qualquer notificação ou outros requisitos regulamentares aplicáveis a tal Incidente de Segurança da Informação. Mediante solicitação do Cliente e às custas do Cliente, no caso de um Incidente de Segurança da Informação, a Infor fornecerá ao Cliente (na medida permitida por lei e sujeito às proteções de confidencialidade aplicáveis) cópias dos registros de atividade dos Sistemas aplicáveis (somente com relação às Informações Incidente de Segurança no que se refere ao Cliente) para uso em qualquer processo legal ou regulatório do Cliente ou em qualquer investigação governamental.

8. Registro e Monitoramento

A Infor monitora seus recursos usados para fornecer Serviços de Subscrição usando um conjunto de ferramentas, configuradas especificamente para gerenciar registros e alertas. Os registros são mantidos física e virtualmente protegidos para evitar adulterações. Informações confidenciais e senhas não são registradas em nenhuma circunstância. Além de capturar informações relacionadas ao serviço, as ferramentas de monitoramento permitem que os administradores acompanhem a atividade do usuário ao entrar e sair do sistema.

9. Segurança de Recursos Humanos

O pessoal da Infor que fornece Serviços de Subscrição está sujeito a obrigações de confidencialidade, está ciente das ameaças e preocupações de segurança da informação, recebe treinamento geral de segurança pelo menos anualmente e está equipado para apoiar as políticas de segurança das informações da organização em geral, bem como em suas funções específicas de trabalho.

10. Controles de Dispositivos Endpoint (Infor Laptops, Workstations e Dispositivos Móveis)

A Infor implementa medidas de segurança consistentes com as práticas geralmente aceitas da indústria para proteção de endpoints, incluindo automação do gerenciamento de patches de aplicativos e sistemas operacionais e proteção antivírus.

11. Devolução e Destruição de Dados

11.1. Devolução

Após a rescisão ou vencimento dos Serviços de Subscrição, a Infor imediatamente disponibilizará todos os Dados do Cliente (dentro de 3-5 dias úteis após o recebimento da solicitação por escrito do Cliente, quem criará um tíquete padrão de Suporte) como exportação de banco de dados nativo fornecido através do serviço de transferência segura de arquivos da Infor. Caso o Cliente exija a devolução dos seus Dados em um formato diferente ou exigir quaisquer outros serviços de assistência à rescisão, a Infor e o Cliente deverão acordar mutuamente com a abrangência desses serviços de assistência a rescisão e com as taxas e despesas a serem pagas por tais serviços.

11.2. Destruição

A Infor excluirá permanentemente todas as instâncias (online ou acessíveis pela rede) de Dados do Cliente dentro de 30 dias após a rescisão ou vencimento dos Serviços de Subscrição. A Infor usará processos padrão geralmente aceitos na indústria para descartar hardware e componentes físicos que contenham Dados do Cliente. Todo o armazenamento é apagado eletronicamente (zerado) antes de ser implantado ou removido do ambiente de produção da Infor.

12. Subcontratados

Os subcontratados da Infor que fornecem bens e serviços à Infor em conexão com os Serviços de Subscrição Infor devem fornecer tais bens e serviços em termos substancialmente semelhantes aos estabelecidos neste ISP. Antes de contratar tal terceiro subcontratado para fornecer qualquer um dos Serviços de Subscrição sob este plano, a Infor examinará tal subcontratado com diligência razoável para ajudar a garantir que tal terceiro possa cumprir essas obrigações de confidencialidade e segurança. A Infor é responsável por todas as ações de seus subcontratados em apoio aos Serviços de Subscrição.

Isenção de responsabilidade: Os seguintes produtos podem ter termos de segurança adicionais ou diferentes: Anael (SaaS) (França), 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), Revenue Mgmt Sys (SaaS), BPCS/LX, XA, System 21 (SaaS).