ACORDO DE QUALIDADE E SEGURANÇA DE TI

Este acordo de qualidade e segurança de TI deverá vigorar como parte do contrato firmado com a Novo Nordisk. ("Contrato"). Ao atualizar o Acordo de Qualidade e Segurança de TI sem atualizar o Contrato, deve ser feita uma referência clara ao título e data de assinatura do Contrato, ou uma cópia do Contrato deve ser anexada. Um caso de CR é sempre necessário, escreva o número de CR aqui.

As notificações diárias relacionadas a este Acordo de Qualidade e Segurança de TI devem ser comunicadas à Novo Nordisk, entrando em contato com a GQ da NN local e com a TI da NN local responsável, ver Anexo [01] para obter informações de contato.

A Novo Nordisk e a empresa prestadora de serviços ("Empresa") são doravante também chamadas individualmente de "Parte" e coletivamente de "Partes".

Considerando que	a Empresa firmou o Contrato com a Novo Nordisk e será doravante também chamada de "Contratada"; e
Considerando que	as Partes deste Acordo desejam estabelecer um Acordo de Qualidade que inclua termos e condições para serviços a serem prestados à Novo Nordisk;
Portanto,	considerando as promessas mútuas no presente e outras considerações boas e valiosas que as Partes reconhecem ser suficientes,

As Partes celebram o seguinte Acordo de Qualidade e Segurança de TI (o "Acordo").

As obrigações contidas neste Acordo sobreviverão até o término do Contrato.

1. PROPÓSITO

Este Acordo de Qualidade e Segurança de TI estabelece requisitos de qualidade e TI para controlar e monitorar o status validado do sistema e a proteção de dados.

Caso haja discrepâncias entre este Acordo de Qualidade e Segurança de TI e o Contrato, as disposições conflitantes serão razoavelmente interpretadas na medida do possível de modo que tais disposições sejam consistentes entre si. Na medida em que tal interpretação consistente não seja razoavelmente possível, os termos do Contrato deverão prevalecer.

1.1 BASE

A base deste Acordo são as Cláusulas Gerais de Segurança de TI da Novo Nordisk atualmente em vigor, o regulamento FDA 21 CFR Parte 11 – Registros Eletrônicos, Assinaturas Eletrônicas, a Orientação PIC/S sobre Boas Práticas para Sistemas Informatizados em Ambientes "BPx" Regulados e a Orientação da FDA para Indústria Parte 11, Registros Eletrônicos; Assinaturas Eletrônicas – Escopo e Aplicação.

	DESCRIÇÃO	Responsabilidade	
		A Contratada	**Novo Nordisk**
2	**SEGURANÇA DE TI GERAL**		
2.1	**Propriedade de dados e Localização de Dados**		
2.1.1	A Contratada concorda que todas as informações a serem gerenciadas, processadas ou armazenadas são informações de propriedade exclusiva ou informações de terceiros confiadas à NOVO NORDISK.	X	
2.1.2	A Contratada deve garantir que os dados da NOVO NORDISK sejam segregados de outros dados de clientes por meio da implementação de controles apropriados.	X	
2.2.1	A Contratada deve ter procedimentos documentados em vigor que regem a gestão de riscos (por exemplo, o impacto das mudanças de infraestrutura) e o tratamento de incidentes de segurança (por exemplo, processo para lidar com incidentes de segurança). Mediante solicitação, estes devem ser compartilhados com a NOVO NORDISK.	X	
2.2.2	A Contratada deve ter um procedimento de escalonamento para gerenciar incidentes de gestão de riscos de informações em vigor.	X	
2.2.3	A Contratada deve informar imediatamente a NOVO NORDISK sobre quaisquer suspeitas de comprometimento relacionadas aos ativos de informações da NOVO NORDISK ou violações de contrato.	X	
2.2.4	A Contratada compromete-se em manter abertura total com a NOVO NORDISK sobre a investigação e as ações subsequentes tomadas após um incidente de segurança.	X	
2.3	**Pessoal do Fornecedor**		
2.3.1	A Contratada deve garantir que o pessoal apropriado possua e seja continuamente treinado em competências de segurança. A Contratada deve ter documentação comprobatória de qualificação e experiência relevantes para o pessoal associado ao serviço realizado para a NOVO NORDISK.	X	
2.3.2	A Contratada deve garantir que as práticas de contratação e investigações de antecedentes de funcionários com acesso privilegiado sejam conduzidas de modo condizente com as melhores práticas e leis relevantes.	X	
2.4	**Segurança Física do Ambiente Operacional**		
2.4.1	O centro de dados da Contratada deve ser certificado e/ou auditado com relação aos padrões do setor por terceiros. A Contratada deve renovar e revisar a certificação ou auditoria anualmente. Os resultados da auditoria não devem conter observações ou achados significativos que foram deixados sem remediação. Os relatórios de auditoria ou as versões do cliente devem ser fornecidos à NOVO NORDISK mediante solicitação. Exemplos de boas práticas são: • ISO 27001 / ISO 27002 • ISAE 3402 • SSAE 16 SOC1 / SOC2	X	

	DESCRIÇÃO	Responsabilidade	
		A Contratada	**Novo Nordisk**
	• Instituto de Tempo de Atividade Nível III / IV • ANSI/TIA-942		
2.5	**Ferramentas e Procedimentos de Segurança**		
2.5.1	A Contratada deve implementar ferramentas de segurança de rede apropriadas para proteger adequadamente os dados e/ou o Sistema de TI da NOVO NORDISK. Os equipamentos de segurança de rede implementados devem ser mantidos, geridos e monitorados de acordo com as melhores práticas. Exemplos de ferramentas de segurança de rede: • Firewalls (FW) • Sistema de Prevenção de Intrusões (IPS) • Sistema de Detecção de intrusões (IDS) • Soluções proxy • Firewall de Aplicativos Web (WAF) • Prevenção de Perda de Dados (DLP)	X	
2.5.2	A Contratada deve garantir que os dados confidenciais, dados pessoais/de privacidade, dados de autenticação ou outros dados confidenciais da NOVO NORDISK estejam protegidos usando mecanismos de criptografia de acordo com as melhores práticas quando estiverem "em repouso" em seus locais de armazenamento. Exemplos de locais de armazenamento de dados onde a criptografia deve ser considerada incluem: • estações de trabalho • servidores • arquivos de configuração • bases de dados • Redes de Área de Armazenamento (SANs) • armazenamento em nuvem (S-3) • fitas de backup • mídia externa (NAS, USB, DVD, HDD)	X	
2.5.3	A Contratada deve manter um programa de Gestão de Chaves para garantir a validade e o sigilo das chaves privadas. O acesso aos principais sistemas de gestão deve ser vigiado e monitorado para atividades suspeitas.	X	
2.5.4	A Contratada deve garantir que software anti-malware, incluindo controle antivírus e de aplicativos, seja instalado em todos os pontos finais aplicáveis (físicos e virtuais), se tecnicamente suportado. Isso inclui sistemas operacionais baseados no Microsoft Windows e no Linux.	X	

	DESCRIÇÃO	Responsabilidade	
		A Contratada	**Novo Nordisk**
2.5.5	A Contratada deve garantir que soluções anti-malware, incluindo controle antivírus e de aplicativos, sejam mantidas e atualizadas com as assinaturas, atualizações e patches atuais. Todos os registros aplicáveis devem ser monitorados para eventos maliciosos.	X	
2.6	**Manutenção e Alterações**		
2.6.1	A Contratada deve garantir que os padrões de segurança de melhores práticas sejam seguidos. Isso inclui, mas não se limita a, ter processos e procedimentos em vigor especificando como a Contratada rege e garante os seguintes requisitos de segurança: • Os acessos são mantidos com os menores privilégios possíveis; • As ações do administrador podem ser rastreadas em uma trilha de auditoria; • O número de pessoas com acesso privilegiado é mantido no mínimo; • Revisão de registros de auditoria selecionados; • Revisão periódica dos acessos do usuário; • As funções do desenvolvedor devem ser separadas das funções de manutenção; • Os relógios do sistema devem ser sincronizados a partir de uma fonte de tempo central;	X	
2.6.2	A Contratada deve garantir que todos os ambientes de produção, desenvolvimento, validação e os ambientes formais de teste sejam mantidos sob configuração e controle de alterações durante toda a duração deste Acordo. Além disso, a Contratada deve garantir que um processo formal esteja em vigor para gerenciar mudanças no Sistema de TI.	X	
2.6.3	A Contratada deve notificar a NOVO NORDISK sobre quaisquer alterações no ambiente da Contratada que possam alterar o nível de risco de informação.	X	
2.6.4	A Contratada deve manter um programa de gestão de ativos que descreva componentes críticos do Sistema de TI. Diagramas precisos e desenhos técnicos devem ser mantidos. A Contratada deve manter um programa de gestão do ciclo de vida para todos os componentes críticos de software e hardware físico.	X	
2.7	**Controle e Autenticação de Acesso**		
2.7.1	A Contratada deve manter um programa de Gestão de Identidade e Acesso para o Sistema ou Serviço de TI. Este programa deve incluir autorização, rastreamento e auditoria de todas as contas e funções para desenvolvimento e pessoal administrativo no ambiente do Sistema de TI.	X	

	DESCRIÇÃO	Responsabilidade	
		A Contratada	**Novo Nordisk**
2.7.2	A Contratada deve garantir que o acesso ao ambiente do Sistema de TI para usuários de *backend* como desenvolvedores, administradores e mantenedores seja estritamente controlado e monitorado. Controles de segurança, como MFA (Autenticação de Fatores Múltiplos), *Privileged Identity Management* (PIM), Firewalls, utilização de conexões *Virtual Private Network* (VPN) e hosts de salto, devem ser considerados.	X	
2.7.3	A Contratada deve fornecer capacidade para configurar o comprimento da senha, a complexidade da senha, o histórico de senhas, a política de bloqueio e a política de redefinição de senha.	X	
2.7.4	A Contratada deve garantir que a política de redefinição de senha e a política de criação de usuários garantam a identidade do solicitante por meio de práticas recomendadas e/ou acordadas pela NOVO NORDISK.	X	
2.7.5	A Contratada deve dar suporte ao uso de MFA e/ou rotação de senha para contas privilegiadas.	X	
2.8	**Registro de Eventos e Monitoramento**		
2.8.1	A Contratada deve garantir que o registro de eventos de segurança selecionados seja realizado, que os registros sejam mantidos e que os registros sejam analisados para identificar possíveis incidentes de segurança. Devem ser mantidos registros devem para a plataforma e para o aplicativo. Os registros de infraestrutura (por exemplo, roteadores, Switches, Proxies, Firewalls) devem ser considerados incluindo infraestrutura em nuvem (por exemplo, registros de AWS Cloud Trail, Azure Activity). Exemplos de eventos de segurança incluem: • acesso legítimo • exceções de autenticação • exceções de autoridade • mudanças de privilégio • ações suspeitas	X	
2.8.2	A Contratada deve garantir que todos os registros estejam protegidos contra adulteração e substituição. Os controles devem proteger contra alterações não autorizadas e problemas operacionais com a instalação que faz o registro.	X	
2.8.3	A Contratada deve garantir que todos os registros do Sistema de TI e infraestrutura sejam coletados, monitorados e analisados de modo centralizado por pessoal de segurança designado usando a solução SIEM.	X	
2.8.4	A Contratada deve manter os registros por um período de tempo definido nos regulamentos e leis aplicáveis ou por acordo com a NOVO NORDISK		
2.8.5	A Contratada deve manter serviços de monitoramento do Sistema de TI que suportam gestão de desempenho, disponibilidade e capacidade. A solução de monitoramento deve ser integrada aos processos de tratamento de incidentes/gestão de incidentes da Contratada.	X	

	DESCRIÇÃO	Responsabilidade	
		A Contratada	**Novo Nordisk**
2.9	**Continuidade de Negócios/Sistemas**		
2.9.1	A Contratada deve garantir que haja planos de backup, restauração e recuperação de desastres (DRP) em vigor para evitar a perda ou a corrupção dos dados da NOVO NORDISK. A localização física geográfica dos backups (no local e fora do local) deve obrigatoriamente ser identificada e aprovada pela NOVO NORDISK.	X	
2.9.2	A Contratada deve garantir que os planos de backup, restauração e recuperação de desastres sejam testados pelo menos anualmente. Um relatório de status mostrando os resultados dos testes deve ser fornecido à NOVO NORDISK mediante solicitação.	X	
2.10	**Gestão de Vulnerabilidades**		
2.10.1	A Contratada deve realizar fortalecimento do sistema para a plataforma e para o aplicativo de acordo com as recomendações do fornecedor de software e/ou as práticas recomendadas do setor (por exemplo, CIS, OWASP, SANS). O fortalecimento do sistema deve ser testado antes da implantação em ambientes de produção.	X	
2.10.2	A Contratada deve garantir que haja um processo contínuo para identificar, avaliar, testar, instalar e gerenciar patches de segurança para todos os softwares de sistema de TI aplicáveis e dispositivos de infraestrutura associados. A varredura de vulnerabilidades deve ser integrada ao processo para verificar e garantir os níveis de patch corretos no Sistema de TI. O processo de correção de segurança deve se integrar aos procedimentos de gestão de mudanças, sempre que possível.	X	
2.10.3	A Contratada deve garantir que os testes de vulnerabilidade e a revisão de código estejam incluídos no ciclo de vida do código de aplicação do Desenvolvimento Seguro.	X	
2.10.4	A Contratada deve garantir que um teste de penetração realizado por terceiros seja conduzido pelo menos uma vez por ano nos componentes de aplicativo, plataforma e/ou infraestrutura.	X	
2.11	**Rescisão ou Expiração do Acordo**		
2.11.1	Em caso de rescisão ou expiração do Acordo, cada parte deve devolver à outra qualquer propriedade da outra que estiver sob sua posse ou controle. A Contratada deve, sem atraso indevido, e no máximo 20 dias úteis após a notificação de rescisão ou expiração do Acordo, fornecer à NOVO NORDISK todos os dados criados até a data da rescisão.	X	

	DESCRIÇÃO	Responsabilidade	
		A Contratada	**Novo Nordisk**
2.11.2	Os dados da NOVO NORDISK devem ser removidos de todas as mídias magnéticas quando a transferência de dados estiver concluída, quando o serviço não for mais fornecido pela Contratada, ou quando o prazo/data para armazenamento de dados acordado for atingido. A Contratada deve garantir que os dados da NOVO NORDISK sejam devidamente destruídos antes do descarte do hardware durante o processo normal do ciclo de vida do sistema.	X	
2.11.3	A Contratada, se GxP, deve seguir as práticas recomendadas do setor para métodos de exclusão de dados. Por exemplo, NIST SP 800-88.	X	
2.11.4	A Contratada, se GxP, deve fornecer à NOVO NORDISK uma cópia de todos os dados de propriedade da NOVO NORDISK mediante solicitação. Os dados serão entregues por meios seguros em um formato padrão usado no setor.	X	
3	**AUDITORIA E INSPEÇÃO**		
3.1	A Novo Nordisk terá direito, mediante notificação prévia razoável, de realizar auditorias/inspeções do sistema de gestão da qualidade da Contratada., funcionários e infraestrutura pertinentes.	X	
3.2	A data e a hora da auditoria serão acordadas no devido tempo e a notificação prévia será fornecida por escrito com ao menos 15 dias úteis de antecedência. Em caso de questões urgentes, a Novo Nordisk terá direito de realizar auditoria da A Contratada mediante notificação prévia por escrito com ao menos 1 (um) dia de antecedência.		X
3.3	Os resultados da auditoria da Contratada pela Novo Nordisk são tratados conforme acordado.	X	
4	**AUTORIZAÇÕES**		
4.1	A Contratada é responsável por solicitar e obter todas as licenças, aprovações regulatórias ou certificados exigidos pelas autoridades para a realização de todas as atividades mencionadas no Contrato;	X	
5	**GESTÃO DA QUALIDADE**		
5.1	A Contratada deve manter um sistema de qualidade, estabelecendo responsabilidades, processos e princípios de gestão de riscos com relação às suas atividades.	X	
5.2	Os desvios do sistema de qualidade e deste acordo de qualidade devem ser documentados e investigados. Devem ser tomadas as ações corretivas e preventivas (CAPA) adequadas.	X	
5.3	A Contratada deve ter um procedimento para lidar com desvios de processos estabelecidos e garantir que os desvios sejam documentados e investigados. Os desvios devem ser seguidos por CAPA suficiente.	X	
5.4	Deve haver sistema de controle de alterações em vigor.	X	

	DESCRIÇÃO	Responsabilidade	
		A Contratada	**Novo Nordisk**
5.5	A Contratada garantirá que todos os funcionários sejam devidamente treinados para que possam desempenhar suas funções de trabalho. O treinamento deve ser documentado.	X	
6	**PROCESSO DE VALIDAÇÃO**		
6.1	A Contratada deve garantir que, antes de um sistema informatizado ser utilizado, seja demonstrado por validação adequada que o sistema seja capaz de alcançar os resultados desejados de forma precisa, consistente e reprodutível.	X	
6.2	A NOVO NORDISK assegurará que, antes de iniciar a fase Piloto, os documentos de TI de suporte sejam elaborados e aprovados. Siga os documentos de TI de suporte envolvidos: - Avaliação do Impacto do Sistema (SIA); - Avaliação de Risco de Segurança de TI; - Plano de Segurança de TI; - Especificação de Exigência do Usuário (URS)		X
6.3	A Contratada garantirá os estudos de validação realizados e todos os documentos de validação finalizados e aprovados para o "Go-live" (ativação) do sistema. Siga os documentos de validação envolvidos: - Avaliação e plano de risco de integridade de dados de TI; - Avaliação de Risco de Qualidade de TI; - Plano de Validação; - Qualificação de Instalação (QI); - Qualificação de Operação (QO); - Qualificação de Desempenho (QD); - Matriz de rastreabilidade; - Relatório de Validação.	X	
6.4	A Contratada deve garantir que os dados só sejam inseridos no sistema ou alterados no sistema por pessoas autorizadas. Isso deve ser protegido por meios físicos ou eletrônicos e protegido contra modificações acidentais ou não autorizadas, periodicamente verificado quanto à acessibilidade e protegido por backups regulares retidos em um local separado e seguro.	X	
6.5	A Contratada realizará Avaliações Periódicas do Sistema seguindo os procedimentos aprovados para garantir que o sistema informatizado seja mantido em estado validado.	X	

ADENDOS:

Distribua os documentos como adendos **sem atualizar o acordo de qualidade ou assinar os acordos**

Adendo 1: Responsável Local de GQ da NN e TI

Nome	Título	Telefone	E-mail
Stefania de Azevedo Fraletti	Coordenador de GQ	+55 11 3868 9165	stdf@novonordisk.com
Laura Fonseca Orlando Azevedo	Gestora de GQ	+55 11 3868 9187	lufo@novonordisk.com
Daniel Penna	Gerente do Sistema de TI	+ 55 11 3868 9213	dapk@novonordisk.com

O Acordo de Qualidade de Segurança de TI é válido “até segunda ordem”.

O Acordo de Qualidade e Segurança de TI será considerado automaticamente encerrado se o Contrato que serve como base para os serviços prestados neste Acordo, for rescindido entre as Partes.

Qualquer disputa com relação a este Acordo de Qualidade e Segurança de TI deve ser resolvida de acordo com os termos estabelecidos no Contrato. O Acordo de Qualidade e Segurança de TI é um apêndice Contrato e é aprovado em conjunto com este.

Portanto, este Acordo de Qualidade e Segurança de TI não é aprovado através de assinaturas separadas, sendo que o responsável de GQ da NN local e o responsável de GQ do Fornecedor confirmam que leram, entenderam e agirão de acordo com os termos deste Acordo de Qualidade e Segurança de TI.