**APÊNDICE – Cláusula de Segurança da informação aos seguintes objetos contratuais: Desenvolvimento de Software, Fornecimento de Software (ex.: sistema ERP), SaaS (Software as a Service), Hospedagem, Software distribuído comercialmente (ex.: pacote Office), Fornecimento de Hardware, Fornecimento de Rede e Monitoramento, Operação, Administração ou Suporte de Sistemas e Aplicativos**

**I) Visando a SEGURANÇA DA INFORMAÇÃO, caberá às PARTES:**

**1. Cada PARTE será única responsável pela seleção, implementação, e manutenção de procedimentos e políticas de segurança que sejam suficientes para garantir que: (i) o uso da conexão de rede por tal parte (e o uso do patrimônio de informações da CONTRATANTE, pela CONTRATADA) seja seguro e utilizado somente para fins autorizados, e (ii) os registros e dados de negócios de tal parte estejam protegidos contra acesso ou uso indevidos, alteração, perda ou destruição.**

**2. Qualquer terceira parte que conecte um dispositivo a uma rede da CONTRATANTE deverá ser autorizada pelo Encarregado de Segurança de TI local. O Fornecedor deverá prover proteção contra o uso externo não autorizado, modificação, divulgação ou destruição, acidental ou intencional, do patrimônio da CONTRATANTE. A terceira parte será responsável pela segurança do dispositivo, através de antivírus e patches, para proteger o patrimônio de informações da CONTRATANTE. Qualquer dispositivo pertencente a uma terceira parte, e que armazene ativos de informações da CONTRATANTE, deverá ser criptografado.**

**2.1. Somente usuários autorizados pela CONTRATANTE poderão acessar as informações e dados contidos na infraestrutura da CONTRATANTE ou na infraestrutura de terceiros contratados ou utilizados pela CONTRATANTE. A CONTRATANTE deverá deter o poder de decisão final, a respeito de quem estará autorizado a acessar os dados e informações, incluindo o próprio pessoal da CONTRATANTE, o pessoal da CONTRATADA, todo o pessoal subcontratado, e qualquer outra terceira parte. Todos os acessos deverão atender às Normas e políticas de tecnologia da informação da CONTRATANTE.**

**2.2. Serão concedidas somente autorizações de acessos individuais (login e senha). Contas genéricas ou compartilhadas são absolutamente proibidas.**

**2.3. Dados ou informações sobre a CONTRATANTE, ou contidos na infraestrutura da CONTRATANTE, quer possuídos, ou cedidos, ou hospedados nas instalações de uma terceira parte, ou na infraestrutura de um Fornecedor de Serviços de Aplicativos, não deverão ser divulgadas a quaisquer terceiras partes, sem a prévia aprovação por escrito da CONTRATANTE.**

**II) Visando a SEGURANÇA DA INFORMAÇÃO, caberá a CONTRATADA:**

**1. Obedecer às normas, procedimentos e Políticas de Tecnologia da Informação da CONTRATANTE, com todos os regulamentos e todas as atualizações correspondentes deste enquadramento, relativas aos países a partir dos quais a CONTRATADA preste os serviços ou hospede aplicativos ou dados.**

**2. Preservar a disponibilidade e precisão das informações dos processos suportados e proteger as informações confidenciais e proprietárias, bem como os direitos de propriedade intelectual da CONTRATANTE.**

**3. Assegurar que o acordo de confidencialidade e as obrigações deste CONTRATO sejam atendidos por seus diretores, funcionários, representantes, agentes, e quaisquer outros subcontratados que irão executar tarefas descritas neste CONTRATO, antes da CONTRATADA direcioná-los à prestação dos serviços objeto deste CONTRATO.**

**3.1. As alterações relativas aos aplicativos, arquitetura, procedimentos operacionais, procedimentos de segurança e sua respectiva avaliação de riscos, deverão ser comunicadas antecipadamente.**

**4. Oferecer a sua máxima cooperação, para permitir que a CONTRATANTE realize a verificação de conformidade dos produtos fornecidos e/ou serviços prestados.**

**5. Atender aos requisitos de governança de tecnologia da informação da CONTRATANTE, o que implica em fornecer informações úteis sobre: (i) infraestrutura / arquitetura de tecnologia da informação e de segurança atualizadas, (ii) organização de tecnologia da informação responsável pelo serviço; e (iii) alterações relativas à arquitetura e procedimentos de segurança, e sua correspondente avaliação de riscos.**

**6. Responsabilizar-se exclusivamente perante o CONTRATANTE sobre todas as considerações de segurança de TI. Sob nenhuma circunstância, a CONTRATANTE assumirá ou aceitará o compartilhamento de responsabilidade entre o Fornecedor e qualquer outra terceira parte, incluindo parceiros de negócios e subcontratados do Fornecedor.**

**7. Assegurar que todas as atividades do serviço mantenham adequadamente os registros de negócios apropriados, de acordo com as melhores práticas da indústria e em conformidade com as leis e regulamentações aplicáveis, e assegurar também que os documentos estejam protegidos contra acesso ou uso indevidos, perda, alteração ou destruição. A CONTRATADA deverá realizar revisões regulares para detectar potenciais problemas de segurança. A CONTRATADA poderá ser obrigada a revelar as configurações, o processo de revisão, e os resultados.**

**8. Responsabilizar-se única e exclusivamente por todas as medidas de segurança para garantir a proteção de seus sistemas e redes internas, isentando a CONTRATANTE de qualquer responsabilidade.**

**9. Responsabilizar-se única e exclusivamente por todas as medidas de segurança para garantir a proteção de seus sistemas e redes internas, isentando a CONTRATANTE de qualquer responsabilidade.**

**10. Juntamente com a definição de requisitos de negócios para novos sistemas ou serviços de informação, ou melhorias em sistemas ou serviços de informação existentes, a CONTRATADA deverá assegurar que a avaliação de segurança seja realizada e que controles de segurança apropriado sejam identificados e incorporados aos requisitos. A avaliação e os controles de segurança a serem incluídos deverão ser analisados e aprovados pela CONTRATANTE.**

**11. Não deverá estabelecer qualquer tipo de link de comunicação de dados entre as suas redes e sistemas e os da CONTRATANTE, incluindo, mas não se limitando a atividades de supervisão, intervenção remota, e qualquer tipo de transferência de dados, por qualquer meio, incluindo, mas não se limitando a links diretos permanentes, Internet, VPN [rede privada virtual], ou dial-up [acesso por linha discada], sem a aprovação da CONTRATANTE.**

**12. Garantir que o ambiente de Tecnologia da Informação, em seu lado, assegure a integridade, disponibilidade e confidencialidade do patrimônio de Tecnologia da Informação da CONTRATANTE, incluindo dados, informações e direitos de propriedade intelectual.**

**12.1. Somente usuários autenticados e autorizados, com uma data de expiração de usuário pré-definida, deverão ter permissão para acessar sistemas da CONTRATANTE e o prazo de acesso deverá ser restrito.**

**12.2. Deverão ser mantidos logs de auditoria completos, nos níveis de conexão, sistema operacional, e aplicativos. A CONTRATANTE se reserva o direito de supervisionar em tempo real, gravar e utilizar os dados armazenados das conexões.**

**12.3. Todas as conexões com a CONTRATADA deverão ser criptografadas e serão estabelecidas somente através de firewalls da CONTRATANTE. Somente serão permitidos hosts e protocolos previamente autorizados.**

**13. Notificar imediatamente a CONTRATANTE, sempre que qualquer funcionário autorizado da CONTRATADA deixe a empresa, ou já não necessite de acesso, ou tenham sido modificadas as responsabilidades para acessar qualquer patrimônio de informações da CONTRATANTE.**

**13.1. Assim que termine a prestação do serviço pela CONTRATADA, por qualquer razão, normal ou anormal, todos os acessos deverão ser imediatamente revogados. A CONTRATADA não será mais autorizada a acessar o patrimônio de informações da CONTRATANTE.**

**13.2. Todas as informações de propriedade da CONTRATANTE deverão ser enviadas à CONTRATANTE, em duas cópias, sendo em seguida removidas com segurança de todos os dispositivos.**

**14. Rever a qualquer tempo o acesso de seus empregados ao patrimônio de informações da CONTRATANTE, e prontamente corrigir qualquer discrepância em potencial. Mediante solicitação da CONTRATANTE, a CONTRATADA deverá revelar os resultados da última análise de acessos, bem como as respectivas ações corretivas.**

**15. Não utilizar qualquer criptografia desenvolvida internamente, para proteger as informações, os aplicativos ou a infraestrutura da CONTRATANTE. Quaisquer algoritmos simétricos, assimétricos, ou de hashing, utilizado na infraestrutura da CONTRATANTE, deverá utilizar algoritmos e ferramentas bem conhecidos, publicados, apresentados à comunidade global de criptografia, e adotados como padrão da indústria.**

**15.1. A resistência dos algoritmos de criptografia deverá ser a mais alta possível, aprovada pelo CSO [Chief Security Officer / Chefe de Segurança] local da CONTRATANTE, e em conformidade com os requisitos de negócios da CONTRATANTE e com a legislação aplicável.**

**15.2. Conexões que utilizem a Internet deverão ser protegidas utilizando tecnologias de criptografia, adotados como padrão de mercado.**

**15.3. Deverão ser criptografados todos os dispositivos móveis e portáteis utilizados para prover o serviço à CONTRATANTE e que contenham dados confidenciais.**

**16. Prover a CONTRATANTE uma lista com os nomes e funções dos funcionários que terão acesso aos Locais da CONTRATANTE. Pessoas incluídas na lista acima referida deverão apresentar-se na recepção do Local da CONTRATANTE, onde receberão um cartão de visitante ou crachá, que deverão portar de forma visível, durante todo o tempo de permanência nas instalações da CONTRATANTE.**

**16.1. Se, por qualquer motivo, uma pessoa não incluída na lista precise acessar o site, ele ou ela deverá ser registrado na recepção, mediante apresentação de sua identificação com foto, ou passaporte. A referida pessoa deverá ser acompanhada por um colaborador da CONTRATANTE, em todos os momentos.**

**16.2. Caso algum membro do pessoal da CONTRATADA, quer previamente autorizado através da lista ou não, necessite acessar áreas sensíveis (tais como salas de servidores, datacenters, armários de rede, etc.), este deverá ser acompanhado por um colaborador da CONTRATANTE, em todos os momentos.**

**16.3. Se a CONTRATADA necessitar acessar os Locais, fora dos horários de trabalho, a CONTRATANTE deverá informar à CONTRATADA as regras específicas a serem respeitadas.**

**17. Designar uma pessoa como responsável pela proteção e descarte seguro dos meios de armazenamento. Caso qualquer mídia de armazenamento precise ser descartada, a CONTRATADA deverá desativá-la de maneira segura, de tal forma que os dados não possam ser recuperados a partir da mesma. A mídia deverá ser descartada utilizando uma terceira parte certificada para realizar descarte seguro, ou destruída fisicamente (após os dados haverem sido apagados) tornando-a completamente inoperante. A desativação / destruição de mídia requer a aprovação prévia da CONTRATANTE e a posterior notificação por esta à CONTRATADA.**

**III) Visando a SEGURANÇA DA INFORMAÇÃO, caberá ao CONTRATANTE:**

**1. Verificar e controlar a qualquer tempo que os produtos fornecidos e/ou serviços prestados pela CONTRATADA estejam em conformidade com o CONTRATO.**

**2. Comunicar à CONTRATADA as regras de segurança estabelecidas em conformidade com a legislação aplicável, bem como as regras de acesso.**

**3. Autorizar antecipadamente, conforme sua conveniência, o uso de qualquer tipo de mídia de armazenamento, com exceção dos discos rígidos internos e fitas de backup. O uso de mídias de armazenamento removíveis e portáteis, tais como CDs, DVDs, drives USB, Flashdrives, etc., é estritamente proibido.**

**4. Autorizar antecipadamente, conforme sua conveniência, todos os ativos de tecnologia da informação da CONTRATANTE que devam deixar as instalações da CONTRATADA (por exemplo, para reparação). Todas as informações armazenadas no dispositivo deverão ser previamente removidas de forma segura. Se a remoção não for prática ou possível, a CONTRATADA será o responsável principal por proteger os ativos contra uso não autorizado, modificação, divulgação, ou destruição, acidental ou intencional.**

**4.1. Previamente à remoção dos ativos das instalações da CONTRATANTE, os controles de segurança a estabelecer deverão ser apresentados pela CONTRATADA e aprovados pela CONTRATANTE.**

**4.2. Se os ativos tiverem de ser desativados ou descartados, as informações deverão ser destruídas de forma segura, e o processo de descarte deverá estar em conformidade com as leis e regulamentos locais.**

**Assim que o serviço prestado termine (vencimento do contrato), a CONTRATADA deverá entregar duas cópias das informações da CONTRATANTE e realizar de forma segura a destruição das informações armazenadas. O acesso deverá ser imediatamente revogado, e a CONTRATADA não será mais autorizado a acessar o patrimônio de informações da CONTRATANTE.**

**O procedimento de autorização para o processo de colocação em produção deverá respeitar as políticas e procedimentos de tecnologia da informação da CONTRATANTE. Os Testes de Aceitação do Usuário (que serão responsabilidade e prerrogativa da CONTRATANTE, independentemente do suporte necessário para realizar estas tarefas) deverão ser realizados antes de qualquer mudança na produção.**