POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
ON TIME TRADUÇÕES ESPECIALIZADAS LTDA.

1. OBJETIVO E ABRANGÊNCIA

1.1. A presente Política de Segurança da Informação ("**Política**") estabelece as diretrizes adotadas pela ON TIME TRADUÇÕES ESPECIALIZADAS LTDA. ("**On Time**") para proteger a confidencialidade, integridade e disponibilidade das informações tratadas no âmbito de suas atividades.

1.2. Esta Política aplica-se a:

(i) **Informações Internas** – dados, documentos, arquivos, memórias de tradução, glossários, modelos, contratos, relatórios e demais informações de titularidade da On Time;

(ii) **Informações de Clientes** – quaisquer documentos, arquivos, dados pessoais ou informações recebidos de clientes ou parceiros para tradução, revisão, formatação ou serviços correlatos; e

(iii) **Informações Operacionais** – conteúdos produzidos, manipulados ou transformados no curso das atividades de tradução, revisão, edição, formatação, juramentação e serviços relacionados.

1.3. Esta Política é obrigatória para todos os Colaboradores Internos e Prestadores Externos que atuem em colaboração com a On Time, exceto para Tradutores Públicos e Intérpretes Comerciais ("**Tradutores Juramentados**").

1.4. Esta Política complementa a legislação aplicável, em especial a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e o Marco Civil da Internet (Lei nº 12.965/2014), bem como os contratos celebrados com clientes e parceiros.

2. DEFINIÇÕES

Para fins desta Política:

2.1. **Colaboradores Internos**: sócios, administradores, diretores, empregados e estagiários da On Time.

2.2. **Prestadores Externos**: pessoas físicas ou jurídicas, sem vínculo empregatício, contratadas pela On Time para a prestação de serviços relacionados ao seu objeto social e que possam acessar Informações Protegidas (tais como tradutores, revisores, editores e diagramadores), excluídos os Tradutores Juramentados.

2.3. **Informações Internas**: todas as informações e dados de titularidade da On Time, inclusive dados financeiros, propostas comerciais, base de clientes, memórias de tradução (TMs), glossários, modelos de documentos, políticas internas, relatórios e comunicações internas.

2.4. **Informações de Clientes**: documentos, arquivos, bancos de dados, e-mails, anexos, dados pessoais ou qualquer outro tipo de informação recebida de clientes, escritórios de advocacia, empresas ou demais parceiros no contexto da prestação de serviços.

2.5. **Informações Protegidas**: conjunto formado pelas Informações Internas e pelas Informações de Clientes, em qualquer formato (físico ou digital, incluindo e-mails, nuvem, mídias removíveis e aplicativos de comunicação).

2.6. **Ambiente de Nuvem Corporativa**: ambiente de armazenamento em nuvem contratado pela On Time, atualmente o **Microsoft 365**, incluindo **SharePoint** e **OneDrive**, ou outro que venha a substituí-lo.

2.7. **Responsável pela Segurança da Informação (RSI)**: pessoa designada pela On Time para coordenar a aplicação desta Política, esclarecer dúvidas, decidir exceções e gerir incidentes de segurança da informação.

2.8. **Responsável pela Tecnologia da Informação (RTI)**: pessoa designada pela On Time para implementar e manter os controles técnicos previstos nesta Política, incluindo gestão de acessos, softwares, nuvem corporativa, antivírus e backups.

3. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

3.1. Na data desta Política, o RSI e o RTI da On Time são exercidos pelo Sr. Fábio Amaral Contente, podendo tais funções ser redistribuídas pela On Time mediante atualização interna.

3.2. O RSI é responsável por:

(i) coordenar a implementação e atualização desta Política;
(ii) esclarecer dúvidas dos Colaboradores Internos e Prestadores Externos;
(iii) aprovar exceções pontuais; e

(iv) conduzir a resposta a incidentes de segurança da informação.

3.3. O RTI é responsável por:

(i) gerenciar perfis e credenciais de acesso;
(ii) instalar e manter softwares corporativos autorizados (por exemplo, Microsoft 365, Trados, ferramentas de OCR etc.);
(iii) administrar o Ambiente de Nuvem Corporativa; e
(iv) implementar antivírus, backups e demais medidas técnicas de proteção.

4. OBRIGAÇÕES DOS COLABORADORES INTERNOS E PRESTADORES EXTERNOS

4.1. Todos os Colaboradores Internos e Prestadores Externos devem:

(i) cumprir integralmente esta Política e demais normas internas da On Time;
(ii) tratar todas as Informações Protegidas como confidenciais;
(iii) utilizar apenas os sistemas, dispositivos e contas autorizados pela On Time;
(iv) zelar para que Informações Protegidas não sejam acessadas por pessoas não autorizadas; e
(v) comunicar imediatamente ao RSI qualquer incidente ou suspeita de incidente de segurança.

4.2. O descumprimento desta Política poderá resultar em:

(i) medidas disciplinares (no caso de Colaboradores Internos); ou
(ii) medidas contratuais (no caso de Prestadores Externos), sem prejuízo de responsabilidade civil e/ou penal, conforme o caso.

5. PRESTADORES EXTERNOS ESPECIAIS – TRADUTORES PÚBLICOS E INTÉRPRETES COMERCIAIS

5.1. Os Tradutores Juramentados, por força de sua atividade regulamentada e sujeita à fé pública, estão vinculados à legislação e às normas das Juntas Comerciais competentes, inclusive no que diz respeito à guarda, arquivamento, sigilo, conservação e expedição de documentos.

5.2. Em razão desse regime jurídico próprio, os Tradutores Juramentados não estão sujeitos integralmente às regras operacionais e tecnológicas previstas nesta Política.

5.3. A On Time envidará seus melhores esforços para celebrar acordos de confidencialidade com os Tradutores Juramentados, com o objetivo de reforçar o dever de sigilo e a confidencialidade das Informações Protegidas, assegurar que os documentos e dados recebidos sejam utilizados exclusivamente para a execução do trabalho solicitado e garantir a comunicação imediata de qualquer incidente de segurança envolvendo documentos encaminhados pela On Time.

6. DADOS PESSOAIS E LGPD

6.1. A On Time trata dados pessoais e, eventualmente, dados pessoais sensíveis contidos em documentos encaminhados por clientes (por exemplo, contratos, petições, relatórios, decisões judiciais etc.).

6.2. O tratamento de dados pessoais pela On Time tem como principais bases legais:

(i) execução de contrato ou de procedimentos preliminares relacionados a contrato de tradução ou serviço correlato;
(ii) cumprimento de obrigação legal ou regulatória; e
(iii) legítimo interesse, quando aplicável, sempre observado o princípio da necessidade.

6.3. Os Colaboradores Internos e Prestadores Externos devem:

(i) coletar e tratar apenas o mínimo de dados pessoais necessário para a execução das atividades;
(ii) evitar cópias desnecessárias de documentos com dados pessoais;
(iii) utilizar preferencialmente o Ambiente de Nuvem Corporativa;
(iv) descartar ou anonimizar dados pessoais quando deixarem de ser necessários, observado o prazo legal ou contratual aplicável; e
(v) comunicar imediatamente ao RSI qualquer incidente envolvendo dados pessoais (perda, extravio, acesso não autorizado, envio indevido etc.).

7. INFORMAÇÕES PROTEGIDAS E CONFIDENCIALIDADE

7.1. Todas as Informações Protegidas são consideradas confidenciais, independentemente de estarem expressamente identificadas como tal.

7.2. É vedado a qualquer Colaborador Interno e/ou Prestador Externo, salvo autorização expressa da On Time:

(i) reproduzir, divulgar, transmitir, publicar ou expor Informações Protegidas;

(ii) utilizar Informações Protegidas para fins pessoais ou alheios aos interesses da On Time ou do cliente;
(iii) armazenar Informações Protegidas em contas, dispositivos ou nuvens não autorizados.

7.3. A On Time poderá, dentro dos limites legais, monitorar o uso de sua infraestrutura tecnológica (e-mail corporativo, nuvem, dispositivos, rede) para fins de segurança da informação, auditoria e apuração de incidentes.

7.4. Ao término do vínculo com a On Time ou a qualquer momento por solicitação, o Colaborador Interno e/ou o Prestador Externo deverá devolver ou excluir todas as Informações Protegidas sob sua guarda, mantendo apenas aquelas que for obrigado a reter por lei ou por contrato, mediante prévia ciência da On Time.

7.5. As obrigações de confidencialidade previstas nesta Política sobrevivem ao término da relação entre o Colaborador Interno e/ou o Prestador Externo e a On Time, por prazo indeterminado, salvo disposição em contrário em contrato específico.

8. MANUSEIO PRÁTICO DAS INFORMAÇÕES

8.1. Os Colaboradores Internos e Prestadores Externos obrigam-se a observar as seguintes diretrizes em relação a documentos que contenham Informações Protegidas:

(i) evitar a impressão de quaisquer documentos que contenham Informações Protegidas, salvo quando estritamente indispensável ao desempenho de seus serviços;
(ii) retirar o documento da impressora imediatamente após a conclusão da impressão, vedada sua permanência desassistida no equipamento;
(iii) todo e qualquer documento físico contendo Informações Protegedias deverá ser armazenado em local seguro, como armário ou gaveta com acesso restrito; e
(iv) documentos físicos que deixarem de ser utilizados deverão ser descartados por meio de fragmentação, rasura ou outro método seguro que impeça integralmente sua leitura ou reconstrução.

8.2. Em transportes, restaurantes, eventos, saguões ou ambientes similares, o Colaborador Interno deve evitar:

(i) abrir documentos com Informações Protegidas em telas visíveis a terceiros;
(ii) discutir detalhes sensíveis em voz alta;
(iii) deixar papéis ou dispositivos desacompanhados.

8.3. O compartilhamento de Informações Protegidas com Prestadores Externos só pode ocorrer:

(i) após formalização de contrato ou termo de confidencialidade; e
(ii) por meio de canais autorizados.

Não obstante o acima, em situações excepcionais de urgência, o RSI poderá autorizar, por escrito (inclusive por e-mail), o envio pontual de documentos a Prestadores Externos ainda em fase de formalização contratual, desde que o Prestador Externo manifeste, também por escrito, compromisso de confidencialidade

9. RECEBIMENTO, ENVIO E COMPARTILHAMENTO DE ARQUIVOS

9.1. Os Colaboradores Internos e os Prestadores Externos são responsáveis por garantir que todo e qualquer arquivo da On Time ou de seus clientes ao qual tenham acesso, bem como aqueles que recebam, armazenem, enviem e/ou compartilhem por meio de contas, dispositivos ou sistemas disponibilizados ou aprovados pela On Time, seja tratado em conformidade com esta Política, com as instruções internas e com a legislação aplicável, respondendo por qualquer uso indevido, divulgação não autorizada, perda, alteração ou destruição decorrente de descumprimento dessas regras.

9.2. É proibido receber, enviar ou compartilhar arquivos que:

(i) não tenham relação com as atividades profissionais da On Time;
(ii) contenham conteúdo pornográfico, violento, racista, discriminatório ou ilícito;
(iii) violem direitos de terceiros (propriedade intelectual, imagem, segredos de negócio); ou
(iv) contenham vírus, malware ou código malicioso.

9.3. É proibido instalar programas ou extensões sem autorização prévia do RTI.

10. ARMAZENAMENTO, NUVEM E EXCEÇÃO PARA TRADOS

10.1. Como regra geral, todos os arquivos de trabalho e Informações Protegidas devem ser armazenados exclusivamente no Ambiente de Nuvem Corporativa da On Time (atualmente SharePoint e/ou OneDrive), ou outro que venha a substituí-los.

10.2. É proibido armazenar documentos de clientes em:

(i) e-mails pessoais;
(ii) contas pessoais de serviços de nuvem; e
(iii) pen drives, HDs externos ou outros dispositivos removíveis, salvo autorização expressa do RSI.

10.3. Exceção – uso de Trados e ferramentas similares

(i) quando estritamente necessário para uso do Trados ou ferramenta semelhante, é permitido o download temporário de arquivos para computadores corporativos da On Time;
(ii) após a conclusão do trabalho, o Colaborador Interno deve salvar a versão final no Ambiente de Nuvem Corporativa e excluir as cópias locais;
(iii) não é permitido armazenar arquivos de clientes em computadores pessoais, mesmo para uso com Trados, salvo autorização excepcional e documentada do RSI.

11. CREDENCIAIS, PERFIS DE ACESSO E SENHAS

11.1. Cada Colaborador Interno terá credenciais de acesso (login e senha) individuais, conforme o perfil definido pelo RTI.

11.2. As credenciais são pessoais e intransferíveis. É proibido:

(i) compartilhar login e senha com terceiros, inclusive outros Colaboradores Internos e/ou Prestadores Externos;
(ii) anotar senhas em locais visíveis ou de fácil acesso;
(iii) utilizar a mesma senha em serviços pessoais e corporativos, sempre que possível.

11.3. O Colaborador Interno deve alterar sua senha imediatamente em caso de suspeita de comprometimento e comunicar o RSI/RTI.

11.4. O RTI poderá definir requisitos mínimos de senha (comprimento, caracteres) e bloquear acessos após tentativas malsucedidas.

12. USO DA INTERNET, E-MAIL CORPORATIVO E APLICATIVOS DE MENSAGENS

12.1. A internet disponibilizada pela On Time deverá ser utilizada exclusivamente para fins profissionais, sendo expressamente vedado ao Colaborador Interno (i) acessar sites ilícitos, com conteúdo impróprio ou que possam comprometer a segurança dos sistemas

da On Time, bem como (ii) realizar o download de programas, aplicativos ou softwares sem a prévia autorização do Responsável por Tecnologia da Informação (RTI).

12.2. Os e-mails corporativos disponibilizados pela On Time são de uso exclusivo para fins profissionais, devendo o Colaborador Interno (i) verificar atentamente os destinatários antes do envio de qualquer mensagem, (ii) evitar o envio de Informações Protegidas para endereços de e-mail externos, salvo quando estritamente necessário, e (iii) sempre que possível, priorizar o envio de links de acesso ao Ambiente de Nuvem Corporativa, em substituição ao envio de anexos de grande volume.

12.3. O uso de aplicativos de mensagens instantâneas, tais como WhatsApp e similares, é permitido exclusivamente para comunicações operacionais relacionadas às atividades da On Time, incluindo prazos, status e alinhamentos, observando-se que (i) o envio de documentos que contenham Informações Protegidas por meio desses aplicativos deverá ser evitado e somente ocorrer em caráter excepcional e quando estritamente necessário, hipótese em que o Colaborador Interno deverá, sempre que possível, salvar o arquivo no Ambiente de Nuvem Corporativa e excluir o referido arquivo do aplicativo e do dispositivo após o uso, e (ii) é expressamente proibido o envio de conteúdo ofensivo, discriminatório, ilícito ou alheio às atividades da On Time.

13. DISPOSITIVOS

13.1 Os dispositivos corporativos disponibilizados pela On Time, incluindo computadores e equipamentos similares, são de sua exclusiva propriedade e poderão ser monitorados, dentro dos limites legais aplicáveis, para fins de segurança da informação, devendo permanecer protegidos por senha e com software antivírus ativo, bem como ser bloqueados sempre que o usuário se afastar do equipamento.

13.2 É vedada a utilização de notebooks pessoais para o armazenamento ou tratamento de Informações Protegidas, salvo no caso de Prestadores Externos formalmente contratados, previamente autorizados pelo Responsável pela Segurança da Informação (RSI) e que atendam, no mínimo, aos seguintes requisitos: (i) dispositivo protegido por senha ou biometria e (ii) antivírus devidamente atualizado.

13.3 A utilização de celulares pessoais é permitida para acesso ao e-mail corporativo e a aplicativos expressamente autorizados pela On Time, desde que tais dispositivos estejam protegidos por senha ou biometria, devendo quaisquer arquivos de clientes eventualmente acessados ou recebidos ser excluídos do dispositivo após o uso.

14. SOFTWARES, ANTIVÍRUS E BACKUPS

14.1. A On Time utiliza somente softwares licenciados, incluindo a suíte Microsoft 365, ferramentas de tradução assistida (CAT) e demais soluções tecnológicas previamente aprovadas pelo RTI.

14.2. É proibido instalar softwares piratas ou não autorizados.

14.3. O RTI é responsável por:

(i) instalar e manter software antivírus em todos os computadores corporativos;
(ii) garantir que o antivírus permaneça ativo e atualizado;
(iii) realizar ou coordenar backups periódicos das informações armazenadas no Ambiente de Nuvem Corporativa, observando os prazos legais e contratuais.

14.4. É proibido ao Colaborador Interno realizar backups em mídias removíveis (pen drives, HDs externos etc.), salvo autorização expressa do RSI.

15. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

15.1. Consideram-se incidentes de segurança, entre outros:

(i) perda, roubo ou extravio de dispositivos com acesso a contas corporativas;
(ii) envio de documentos a destinatários incorretos;
(iii) suspeita de vírus, malware ou acesso não autorizado;
(iv) vazamento, exposição indevida ou exclusão acidental de arquivos de clientes armazenados no Ambiente de Nuvem Corporativa ou que possam comprometer a entrega ao cliente.

15.2. Em qualquer dessas hipóteses, o Colaborador Interno deve:

(i) comunicar imediatamente o RSI; e
(ii) seguir as orientações do RSI para contenção e remediação.

15.3. O RSI avaliará a necessidade de informar clientes, titulares de dados ou autoridades competentes, em conformidade com a LGPD e contratos aplicáveis.

16. MONITORAMENTO E AUDITORIA

16.1. A On Time poderá, dentro dos limites legais:

(i) monitorar o uso de sua rede e internet;
(ii) auditar acessos à nuvem corporativa;
(iii) verificar o uso de e-mail corporativo e softwares;
(iv) inspecionar dispositivos corporativos.

16.2. O objetivo do monitoramento é proteger as Informações Protegidas, os sistemas da On Time e os interesses de seus clientes, não havendo expectativa de privacidade no uso de recursos corporativos.

17. SANÇÕES

17.1. O descumprimento desta Política poderá resultar em sanções proporcionais à gravidade da conduta, a serem definidas pela diretoria da On Time, sem prejuízo de medidas legais cabíveis.

17.2. Para Colaboradores Internos, as sanções podem incluir advertência, suspensão e rescisão contratual. Para Prestadores Externos, podem incluir advertência, rescisão contratual e responsabilização por perdas e danos.

18. DISPOSIÇÕES FINAIS

18.1. Exceções às regras desta Política devem ser solicitadas ao RSI, que poderá autorizá-las de forma pontual e registrada.

18.2. Esta Política é autônoma em relação aos contratos firmados com Colaboradores Internos e Prestadores Externos, podendo suas disposições de confidencialidade e segurança sobreviver ao término desses contratos.

18.3. Todos os Colaboradores Internos e Prestadores Externos que tenham acesso a Informações Protegidas deverão formalizar sua ciência e adesão a esta Política por meio de resposta por e-mail corporativo confirmando a leitura e concordância do Anexo I.

18.4. A On Time poderá revisar e atualizar esta Política sempre que necessário, em razão de alterações legais, contratuais, tecnológicas ou de organização interna.

Última atualização: 4/12/2025.

ANEXO I –TERMO DE CIÊNCIA E ADESÃO

TERMO DE CIÊNCIA E ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA ON TIME TRADUÇÕES ESPECIALIZADAS LTDA.

Eu, **[NOME COMPLETO]**, **[nacionalidade]**, **[estado civil]**, **[profissão]**, portador(a) do RG nº **[●]** e CPF nº **[●]**, atuando na qualidade de **[empregado(a) / estagiário(a) / prestador(a) de serviços]** da **ON TIME TRADUÇÕES ESPECIALIZADAS LTDA.** ("On Time"), DECLARO, para todos os fins de direito, que:

a) recebi, li integralmente e compreendi o conteúdo da Política de Segurança da Informação da On Time ("Política");

b) estou ciente de que, no exercício das minhas atividades, poderei ter acesso a Informações Protegidas da On Time e de seus clientes e parceiros, comprometendo-me a observar integralmente as regras de confidencialidade e segurança previstas na Política;

c) comprometo-me a cumprir todas as obrigações constantes da Política, inclusive quanto às restrições ao download e armazenamento de documentos em dispositivos não autorizados; e

d) tenho ciência de que o descumprimento da Política poderá sujeitar-me às sanções disciplinares, civis, trabalhistas e/ou contratuais cabíveis, conforme a natureza de minha infração e da minha relação com a On Time.

São Paulo, [data]

[NOME COMPLETO]
[empregado(a) / estagiário(a) / prestador(a) de serviços]