



ASSURANCE IT

**POL04 - Política de Segurança da
Informação e Privacidade
de Dados**

MENSAGEM DOS SÓCIOS FUNDADORES

Para todos os colaboradores da Empresa. Nos últimos anos a ASSURANCE IT vem se estruturando para atuar diante da expansão do mercado Tecnologia no Brasil através da implementação de sólidos processos e políticas de governança corporativa.

O dinamismo no segmento de TI abre caminhos para uma profunda transformação com impacto na vida de milhões de brasileiros que passarão a ter cada vez mais acesso aos serviços ligados a tecnologia. Transformação que se inicia ainda enquanto vivenciamos a maior crise sanitária da nossa época, a pandemia de Covid-19.

Temos respondido a todos os desafios impostos por este momento de maneira sólida e estruturada, resultado de um modelo de negócio resiliente, socialmente responsável e com alto impacto ESG (sigla em inglês para Ambiental, Social e Governança).

Nossos Valores – “Agir com integridade”, “Atuar com segurança”, “Garantir a excelência operacional”, “Compromisso com o cliente”, “Orientação para resultados” e “Respeito às pessoas” – nos orientam a conduzir nossos negócios e todos os nossos relacionamentos com os mais altos padrões de integridade e no total cumprimento de todas as legislações e regulamentações aplicáveis às nossas atividades. Temos uma abordagem de tolerância zero a comportamento antiético, discriminação e atos de corrupção.

Nosso Código de Conduta Ética Profissional define os princípios e as normas básicas a serem adotadas por todos os funcionários da ASSURANCE IT e está sempre em evolução, acompanhando a realidade do nosso setor e das nossas operações. Estar em conformidade com o Código é uma responsabilidade de cada um. Assim, é fundamental que você o leia com atenção, como exercício para a prática rotineira de seus conceitos e princípios.

Em caso de dúvida, encaminhe suas questões ao seu superior imediato ou ao Comitê de Compliance através do seguinte canal:

legalcompliance@assuranceit.com.br

comitedeetica@assuranceit.com.br

diretoria@assuranceit.com.br

Agradecemos por sua dedicação e por seu comprometimento em praticar e defender os princípios de conduta ética no dia a dia de nossas operações.

Atenciosamente,

Raul Hallak, Robson Pereira e Rodrigo Grodzicki

1. INTRODUÇÃO

A Política de segurança da informação, na ASSURANCE IT, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Companhia, ou acesso a informações pertencentes à ASSURANCE IT. Todo e qualquer usuário de recursos computadorizados da Companhia tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

- Exponha a Companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.
- Envolver a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Envolver o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

2. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da ASSURANCE IT.

3. MISSÃO DO SETOR DE TECNOLOGIA DA INFORMAÇÃO.

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da ASSURANCE IT. Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

4. É DEVER DE TODOS NA ASSURANCE IT.

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a ASSURANCE IT e deve sempre ser tratada profissionalmente.

5. CLASSIFICAÇÃO DA INFORMAÇÃO.

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

- 1 – Pública
- 2 – Interna
- 3 – Confidencial
- 4 – Restrita

Conceitos sobre Informação:

- Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.
- Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
- Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem ou operacional ao negócio da organização ou ao negócio do parceiro.
- Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

6. DADOS DOS FUNCIONÁRIOS

A ASSURANCE IT se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução do seu negócio. Todos os Dados Pessoais de Funcionários que porventura sejam armazenados serão considerados dados confidenciais. Dados Pessoais de Funcionários sob a responsabilidade da ASSURANCE IT não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da ASSURANCE IT. Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da empresa, sem prévia e expressa autorização por parte da diretoria.

Mesmo que seja autorizado o armazenamento destes dados, ASSURANCE IT não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos Servidores de empresa, e jamais poderão fazer parte da rotina de backup da empresa.

7. ADMISSÃO E DEMISSÃO DE FUNCIONÁRIOS / TEMPORÁRIOS / ESTAGIÁRIOS

O setor de Recrutamento e Seleção de Pessoal da Companhia deverá informar ao setor de Informática, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da Companhia. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo setor de Informática.

Cabe ao setor solicitante da contratação a comunicação ao setor de Informática sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço à Companhia, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema. No caso de demissão, o setor de Recursos Humanos deverá comunicar o fato o mais rapidamente possível à Informática, para que o funcionário demitido seja excluído do sistema.

Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da ASSURANCE IT. Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política através do termo de consentimento que deverá ser assinado digitalmente no ato do ingresso a nas respectivas atualizações desta política.

8. TRANSFERÊNCIA DE FUNCIONÁRIOS / TEMPORÁRIOS / ESTAGIÁRIOS

Quando um funcionário for promovido ou transferido de seção ou gerência, o setor de cargos e salários deverá comunicar o fato ao Setor de Informática, para que sejam feitas as adequações necessárias para o acesso do referido funcionário ao sistema informatizado da Companhia.

9. PROGRAMAS ILEGAIS

A ASSURANCE IT respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de programas ilegais (Sem licenciamento) na ASSURANCE IT.

Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da Companhia, mesmo porque somente o pessoal da área de Ti tem autorização para instalação de programas previamente autorizados dentro da política de segurança da companhia. Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores.

Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados, se responsabilizam perante a companhia por quaisquer problemas ou prejuízos causados oriundos desta ação, estado sujeitos as sanções previstas neste documento.

10. PERMISSÕES E SENHAS

Todo usuário para acessar os dados da rede da ASSURANCE IT, deverá possuir um login e senha previamente cadastrados pelo pessoal de TI.

Quem deve fornecer os dados referentes aos direitos do usuário é o responsável direto pela sua chefia, que deve preencher uma ficha e entregá-la ao departamento de RH. Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da Companhia, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de TI, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

A área de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro login e após isso a cada 45 (quarenta e cinco) dias. Por segurança, a área de TI recomenda que as senhas tenham sempre um critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc.) deverão comunicar ao Setor de TI qual será o seu substituto quando de sua ausência da ASSURANCE IT, para que as permissões possam ser alteradas (delegação de poderes). Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pelo pessoal de TI.

11. COMPARTILHAMENTO DE DADOS

Não é permitido o compartilhamento de pastas nos computadores e desktops da empresa. Todos os dados deverão ser armazenados nos Servidores da rede, e a autorização para acessá-los deverá ser fornecida pelo Servidor AD (Active Directory). O Pessoal de TI está orientado a periodicamente todos os compartilhamentos existentes nas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam armazenados na rede.

Os compartilhamentos de impressoras devem estar sujeitos às autorizações de acesso do AD. Não é permitido na ASSURANCE IT o compartilhamento de dispositivos móveis tais como pen-drivers e outros.

12. BACKUP (COPIA DE SEGURANÇA DOS DADOS)

Todos os dados da ASSURANCE IT deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade do Setor Interno de TI e deverão ser feitas diariamente. Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, do Sistema de Gestão da ASSURANCE IT.

Esta cópia será feita imediatamente após a comunicação formal da Contabilidade, por meio de memorando, que o referido mês foi encerrado. Nos meses pares, a Informática enviará 1 (uma) cópia extra da fita do "backup" de fechamento do referido mês, para ser arquivada na Contabilidade.

As cópias deverão ser feitas em mídias removíveis e deverão abranger todos os dados da empresa, que deverão estar nos servidores. As cópias deverão ser protegidas por senhas para evitar que pessoas não autorizadas tenham acesso a estes dados em caso de perda ou roubo da mídia.

As Cópias deverão ser feitas de forma escalonada em Mídias diferentes para cada dia da semana. As mídias deverão ser armazenadas em local seguro, fora das instalações do CPD para evitar perda de dados em casos sinistros. Semanalmente, no final do expediente de sexta feira um conjunto de backup deverá ser enviado para um local externo em outro endereço a ser definido pela diretoria. Neste local deverá haver permanentemente um conjunto completo de backup capaz de restaurar todos os dados da ASSURANCE IT em caso de sinistro.

O conjunto de backup armazenado externamente deverá sofrer rodízio semanal com um dos conjuntos de backup ativo. Validação do Backup – Mensalmente o backup deverá ser testado pelo pessoal de TI, voltando-se parte ou todo o conteúdo do backup em um HD previamente definido para este fim. Esta operação deverá ser acompanhada pelo Gerente da ASSURANCE IT responsável por supervisionar a área de TI.

13. CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS

Não é política da ASSURANCE IT o armazenamento de dados em desktops individuais, entretanto, existem alguns programas fiscais que não permitem o armazenamento em rede. Nestes e em outros casos, o pessoal de TI deverá alertar ao usuário que ele deve fazer backup dos dados do seu equipamento periodicamente.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da ASSURANCE IT.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da ASSURANCE IT o Setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

14. SEGURANÇA E INTEGRIDADE DOS DADOS

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de TI, assim como a manutenção, alteração e atualização de equipamentos e programas.

15. PROPRIEDADE INTELECTUAL

É de propriedade da ASSURANCE IT, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a ASSURANCE IT.

16. PROPRIEDADE INTELECTUAL

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na ASSURANCE IT. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados. O uso da Internet será monitorado pelo Setor de Informática, inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da Direção da Companhia, com base em recomendação do Supervisor de Informática. Não é permitido instalar programas provenientes da Internet nos microcomputadores da ASSURANCE IT, sem expressa anuência do setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da ASSURANCE IT;
- Que promovam discussão pública sobre os negócios da ASSURANCE IT, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível “Confidencial”.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

17. USO DO CORREIO ELETRÔNICO (E-MAIL)

O correio eletrônico fornecido pela ASSURANCE IT é um instrumento de comunicação interna e externa para a realização do negócio exclusivos da ASSURANCE IT. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da ASSURANCE IT, não podem ser contrárias à legislação vigente e nem aos princípios éticos da ASSURANCE IT.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;

- Sejam hostis e inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas da ASSURANCE IT.

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico o Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Não será permitido o uso de ferramentas gratuitas de e-mail (liberados em alguns sites da web), nos computadores da ASSURANCE IT. O Setor de Informática poderá, visando evitar a entrada de vírus na ASSURANCE IT, bloquear o recebimento de e-mails provenientes de sites gratuitos.

18. NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

O Setor de Informática é responsável pela aplicação da Política da ASSURANCE IT em relação a definição de compra e substituição de “software” e “hardware”. Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática. Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

19. USO DE LAP TOPS (COMPUTADORES PESSOAIS) NA ASSURANCE IT

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade da ASSURANCE IT, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido. Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao Setor de Informática;
- Envie uma cópia da ocorrência para o Setor de Informática.

20. RESPONSABILIDADE DOS GERENTES / SUPERVISORES

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da Companhia, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O Setor de Informática fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Que informação ou rotina determinado usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

21. SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos e aos celulares da ASSURANCE IT, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de Informática, de acordo com as definições da Diretoria da ASSURANCE IT. Ao final de cada mês, para controle, serão enviados relatórios informando a cada gerência quanto foi gasto por cada ramal.

22. USO DE ANTIVÍRUS

Todo arquivo em mídia proveniente de entidade externa à ASSURANCE IT deverá ser verificado por programa antivírus. Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

23. PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

Considerando que os empregados da ASSURANCE IT têm acesso irrestrito as informações sigilosas da empresa, tais como: lista de clientes, contratos assinados, banco de dados, valores financeiros, dentre outras estratégias comerciais;

Considerando que por vezes tomamos conhecimento de que empregados de outras empresas se utilizam destas informações de maneira equivocada;

E considerando as consequências a que está sujeito o empregado que faz uso indevido destas informações, analisaremos a seguir estas consequências.

1 – Em primeiro lugar temos a situação prevista no artigo 482, letra “c”, da Consolidação das Leis do Trabalho – CLT que, acaso configurada, poderá ensejar a demissão por justa causa do empregado faltoso:

“Art. 482. Constituem justa causa para rescisão do contrato de trabalho pelo empregador:

(...)

c) negociação habitual por conta própria ou alheia sem a permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço;”

Na prática, caso a ASSURANCE IT tome conhecimento de que algum empregado vem negociando, de forma habitual, com alguma empresa concorrente, ou até mesmo que este empregado tenha aberto um negócio próprio, objetivando fazer concorrência com a ASSURANCE IT, bem como esteja se utilizando de segredos comerciais que somente teve acesso em virtude da profissão exercida dentro da ASSURANCE IT, também objetivando fazer concorrência com a ASSURANCE IT, tais atitudes caracterizarão a concorrência desleal, podendo, por conseguinte, ser o empregado demitido por justa causa, perdendo direito ao

13º salário proporcional, férias proporcionais acrescidas de 1/3, aviso prévio e a multa de 40% sobre os depósitos do FGTS.

2 – Em segundo lugar, além do disposto na CLT, a legislação brasileira vigente, mais especificamente a Lei nº 9.279/1996 – Lei de Propriedade Intelectual dispõe, em seu artigo 195, inciso XI, que:

“Art. 195. Comete crime de concorrência desleal quem:

(...)

XI – divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

(...)

Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.”

Por exemplo, copiar banco de dados para venda ou uso próprio. Neste caso, além de estar sujeito a uma demissão por justa causa, poderá responder criminalmente pelo uso indevido das informações sigilosas a que teve acesso durante o período para o qual trabalhou para a ASSURANCE IT.

Diante disto e, apesar de felizmente não termos nos deparado até o presente momento com qualquer situação que ensejasse a adoção das medidas acima mencionadas, servimo-nos da presente para cientificar todos os empregados da ASSURANCE IT acerca das consequências a que estarão sujeitos, caso pratiquem concorrência desleal face à empresa, enquanto empregados desta empresa ou caso se utilizem de segredos comerciais a que tiveram acesso em virtude do trabalho efetuado, durante o contrato de trabalho ou até mesmo depois de rescindido, podendo responder, inclusive, criminalmente pelo uso indevido de tais informações.

24. Alterações

O Conselho de Administração revisa e aprova este Código pelo menos uma vez ao ano e é o responsável final pelo controle do cumprimento deste Código.

25. Informações de Contato

CONTATOS INTERNOS

E-mail: comitedeetica@assuranceit.com.br

CONTATO DA AREA DE TI

E-Mail: suporte@assuranceit.com.br

Telefone: (11) 37367215

CONTATOS INTERNOS COMITÊ DE ÉTICA

Av. Dr Cardoso de Melo, 1460 – 7andar, Vila Olimpia, São Paulo, SP - CEP: 04548-005

Gestão de Pessoas

Ademir Oliveira– Telefone: (11) 37367213

E-mail: ademir.oliveira@assuranceit.com.br

Maira Vieira – Telefone: (11) 37367213

E-mail: maira.vieira@assuranceit.com.br

Thainara Cabral – Telefone: (11) 37367213

E-mail: thainara.cabral@assuranceit.com.br

Sócios Diretores

Robson Vieira Pereira Telefone: (11) 37367200

E-mail: robson.pereira@assuranceit.com.br

Rodrigo Grodzicki – Telefone: (11) 37367204

E-mail: rodrigo@assuranceit.com.br

Raul Hallak -Telefone: (11) 37367205

E-mail: raul.hallak@assuranceit.com.br

26. Termo de Consentimento para Tratamento de Dados Pessoais

Todos os colaboradores deverão estar cientes e assinar o Termo de Consentimento para o Tratamento de Dados Pessoais visando registrar a manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus dados pessoais para finalidade específica, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Dados Pessoais

O Controlador fica autorizado a tomar decisões referentes ao tratamento e a realizar o tratamento dos seguintes dados pessoais do Titular:

- Nome completo.
- Nome Social;
- Nome empresarial;
- Filiação;
- Data de nascimento;
- Número e imagem do documento de identificação (RG/CNH/CTPS etc);
- Número e imagem do Cadastro de Pessoas Físicas (CPF);
- Número do Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- Número e imagem da Carteira Nacional de Habilitação (CNH);
- Fotografia 3x4;
- Dados e Imagem da Certidão de Nascimento ou Casamento;
- Estado civil;
- Número e imagem do Certificado militar – reservista;
- Nível de instrução ou escolaridade;
- Dados e Imagem Diploma de Conclusão do Ensino médio e /superior;
- Dados e Imagem do Certificado do Ensino médio, Cursos de Especialização e/ superior;
- Dados Históricos profissionais fornecidos pelo Titular;
- Endereço completo e comprovante de Residência;
- Números de telefone, WhatsApp e endereços de e-mail;
- Exames, atestados e laudos médicos;
- Banco, agência e número de contas bancárias;
- Nome de usuário e senha específicos para uso dos sistemas do Controlador;
- Comunicação, verbal e escrita, mantida entre o Titular e o Controlador;
- Biometria. (Acesso a empresa e Ponto Biométrico).

Finalidades do Tratamento dos Dados

O tratamento dos dados pessoais listados neste termo tem as seguintes finalidades:

- Possibilitar que o Controlador identifique e entre em contato com o Titular para fins de relacionamento comercial.
- Possibilitar que o Controlador elabore contratos comerciais com o Titular.
- Possibilitar que o Controlador envie ou forneça informações profissionais contidas no Resumo Profissional (Currículo) do Titular á Clientes e Parceiro do Controlador para fins de prestação de serviços.

Compartilhamento de Dados

O Controlador fica autorizado a compartilhar os dados pessoais do Titular com outros agentes de tratamento de dados, caso seja necessário para as finalidades listadas neste termo, observados os princípios e as garantias estabelecidas pela Lei nº 13.709.

Segurança dos Dados

O Controlador responsabiliza-se pela manutenção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Em conformidade ao art. 48 da Lei nº 13.709, o Controlador comunicará ao Titular e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao Titular.

Término do Tratamento dos Dados O Controlador poderá manter e tratar os dados pessoais do Titular durante todo o período em que os mesmos forem pertinentes ao alcance das finalidades listadas neste termo. Dados pessoais anonimizados, sem possibilidade de associação ao indivíduo, poderão ser mantidos por período indefinido. O Titular poderá solicitar via e-mail ou correspondência ao Controlador, a qualquer momento, que sejam eliminados os dados pessoais não anonimizados do Titular. O Titular fica ciente da impossibilidade de manter a relação comercial com o Controlador a partir da eliminação dos dados pessoais.

Direitos do Titular

O Titular tem direito a obter do Controlador, em relação aos dados por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei nº 13.709; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei nº 13.709; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º da Lei nº 13.709.

Direito de Revogação do Consentimento

Este consentimento poderá ser revogado pelo Titular, a qualquer momento, mediante solicitação via e-mail ou correspondência ao Controlador.

27. Notificação ao Leitor

A Empresa se reserva o direito de, no todo ou em parte, modificar, suspender ou revogar este Código e quaisquer políticas relacionadas, procedimentos e programas a qualquer tempo. A Empresa também se reserva o direito de interpretar e alterar este Código e suas políticas segundo seu próprio critério. Quaisquer alterações ao presente Código serão divulgadas e relatadas conforme exigido por lei.

A Empresa emprega Funcionários sindicalizados. Se este Código conflitar com uma previsão específica de um acordo ou convenção coletiva que rege salários, termos e/ou condições de trabalho para Funcionários que fazem parte ou são representados por sindicatos, o acordo ou convenção coletiva prevalecerá sobre este Código. Se um acordo ou convenção coletiva for omissa em relação a alguma parte deste Código, ou se este Código suplementa um acordo ou convenção coletiva, os Funcionários que fazem parte ou são representados por sindicatos devem respeitar este Código.

Nem este Código, nem quaisquer políticas mencionadas pelo mesmo, conferem quaisquer direitos, privilégios ou benefícios a Funcionário, ou criam direito de manutenção do vínculo empregatício com a Empresa, estabelecem condições empregatícias ou criam, expressa ou implicitamente, vínculo empregatício de qualquer espécie entre Funcionários e a Empresa. Além disso, este Código não modifica o vínculo empregatício entre os Funcionários e a Empresa.

Este Código está divulgado no nosso website e/ou intranet. A versão do presente Código divulgada no nosso website e/ou intranet poderá estar mais atualizada e substitui qualquer versão impressa no caso de haver alguma discrepância entre a versão impressa e o que estiver disposto no nosso website e/ou na intranet.

<https://www.assuranceit.com.br>

<https://www.assurance.com.br/workplace/consultor/>

28. Controle e Histórico de Versões

Data	Versão	Sumario
Julho/2012	1/2012	Criação do instrumento
Julho/2013	1/2013	Revisão geral do instrumento
Julho/2014	1/2014	Revisão geral do instrumento
Julho/2015	1/2015	Revisão geral do instrumento
Julho/2016	1/2016	Revisão geral do instrumento
Julho/2017	1/2017	Revisão geral do instrumento
Julho/2018	1/2018	Revisão geral do instrumento
Julho/2019	1/2019	Revisão geral do instrumento
Julho/2020	1/2020	Revisão geral do instrumento
Julho/2021	1/2021	Revisão geral do instrumento
Julho/2022	1/2022	Revisão geral do instrumento