POLÍTICA INTERNA DE SEGURANÇA DA INFORMAÇÃO

Comitê de Segurança da Informação

SFA DO BRASIL

systems for automation

POLÍTICA INTERNA DE SEGURANÇA DA INFORMAÇÃO DA SFA DO BRASIL

I. INTRODUÇÃO

Este documento foi elaborado visando implementar as orientações das mais atualizadas e confiáveis diretrizes de segurança, em especial as normas NBR ISO IEC 27001, NBR ISO IEC 27002, NBR ISO IEC 15408, e outros, tendo por finalidade atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso, penalidades, e criar uma cultura educativa empresarial de proteção aos dados da SFA DO BRASIL.

A justificativa da necessidade de implementação da presente Política se faz ainda mais evidente, tendo em vista que a SFA DO BRASIL é uma empresa nacional prestadora de serviço de automatização de processos cotidianos em todas as áreas das empresas.

II. OBJETIVO

O objetivo deste documento é estabelecer as diretrizes e regras de Segurança da Informação, em relação à manipulação de informações e utilização da infraestrutura tecnológica da SFA DO BRASIL, de acordo com princípios éticos e legais.

São também objetivos deste documento:

a) Padronizar as atividades de segurança para o uso e administração dos recursos da Tecnologia da Informação;

b) Fornecer suporte às atividades de segurança que visem garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações;

c) Assegurar que os recursos humanos e tecnológicos comprometidos com o manuseio e processamento da informação estão de acordo com as presentes regulamentações.

d) Corroborar regras estabelecidas no Código de Ética e Conduta de Negócio e Política Anticorrupção da SFA DO BRASIL.

1. **DEFINIÇÕES**

Além de outras definidas nesta Política as seguintes expressões ou termos terão o significado que lhes é a seguir atribuído (utilizadas no plural ou no singular):

- USUÁRIO ou USUÁRIOS: significa qualquer funcionário ou prestador de serviços que utilizem o ambiente da SFA DO BRASIL para o desenvolvimento de suas atividades.

- INFORMAÇÃO ou INFORMAÇÕES: significa como o patrimônio da SFA DO BRASIL, consistente nas suas informações, que podem ser de caráter comercial, estratégico, técnico, financeiro, mercadológico, legal, de recursos humanos, ou de qualquer outra natureza, não importando se protegidas ou não de confidencialidade, desde que se encontrem armazenadas e/ou trafegadas na infraestrutura tecnológica da SFA DO BRASIL.

- SEGURANÇA DA INFORMAÇÃO: por sua vez, deve ser entendido como a adoção de medidas eficazes para resguardar que as informações da SFA DO BRASIL e de seus clientes e fornecedores, sejam conhecidas somente por aqueles que devem conhecê-las, evitando seu uso indevido, inadequado, ilegal, ou em desconformidade com esta Política Interna de Segurança da Informação.

2. **COMPROMISSO DOS USUÁRIOS**

A presente Política Interna de Segurança da Informação constitui um conjunto de normas e regras de Segurança da Informação a possibilitar o processamento, compartilhamento e armazenamento de informações da SFA DO BRASIL e de seus clientes e fornecedores, através de sua infraestrutura tecnológica e deve ser respeitado por todos os usuários, pois trará efeitos obrigacionais nos termos desta Política e da legislação vigente.

Todos os usuários são responsáveis por cumprir e fazer cumprir as regras, normas e procedimentos estabelecidos nesta Política de Segurança da Informação.

Esta Política Interna de Segurança da Informação é destinada a todos os USUÁRIOS.

3. **COMPROMISSO DO DEPARTAMENTO DE RECURSOS HUMANOS**

É compromisso do RH quando um funcionário for contratado, promovido ou transferido de departamento ou gerência, solicitar a assinatura do termo de responsabilidade e comunicar o fato a Gestão de TI Corporativa via formulário padrão para que sejam feitas as adequações necessárias para o acesso do referido funcionário ao sistema informatizado da SFA DO BRASIL.

Também é compromisso do RH informar, via e-mail corporativo, todas as alterações (contratação ou desligamento), transferência de funcionários entre setores ou funções, imediatamente após a sua efetivação

4. **COMPROMISSO DA TI**

Manter relatórios atualizados quanto ao correto uso da estrutura informatizada da empresa.

5. **COMITÊ DE SEGURANÇA DA INFORMAÇÃO**

Criou-se um COMITÊ DE SEGURANÇA DA INFORMAÇÃO, que é o órgão permanente que conduzirá toda a gestão da presente Política Interna de Segurança da Informação e será representado pelo Líder da Segurança da Informação.

Tal Comitê será necessariamente composto pelo RH, TI e Governança e Infraestrutura, que constitui de um grupo de trabalho para tratar de questões ligadas à Segurança da Informação e propor soluções específicas, que envolvam direta ou indiretamente a SFA DO BRASIL. O Comitê será responsável pela análise de todas as infrações cometidas pelos usuários a presente Política, devendo gerar um relatório que pondere acerca da gravidade e riscos sob o enfoque técnico e legal de cada infração cometida, culminando na recomendação de processo administrativo disciplinar para apuração dos fatos e aplicação das ações disciplinares cabíveis, para eventual e futuro encaminhamento às autoridades policiais e/ou judiciais, quando necessário.

Portanto, todo e qualquer evento que coloque em risco a Segurança da Informação da SFA DO BRASIL, assim como quaisquer outros incidentes relacionados que violem a presente Política, deverão ser comunicados, de imediato, pelo suporte ou por qualquer usuário que tenha conhecimento do mesmo, a Infraestrutura para que analise e recomende as medidas necessárias, sendo que, na omissão ou inércia daquele que tiver

ciência, ou que desconfie da ocorrência de incidente relacionado à Segurança da Informação, este será responsabilizado na medida de sua omissão.

O COMITÊ DE SEGURANÇA DA INFORMAÇÃO poderá ser contatado a qualquer momento pelos usuários para esclarecer dúvidas, obter orientações, expressar opiniões, reportar situações de violação a presente Política e outros, através da conta de e-mail compliance@sfadobrasil.com.br

Sugestões que visem aumentar o nível de Segurança da Informação deverão ser encaminhadas ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO para que este proceda à análise valorativa destas iniciativas, apresentando um parecer à Diretoria no prazo máximo de 30 (trinta) dias do recebimento da sugestão, opinando ou não pela sua aprovação e posterior implementação.

É também atribuição do COMITÊ DE SEGURANÇA DA INFORMAÇÃO a coordenação da comunicação e divulgação institucional desta Política, podendo recomendar as medidas que entender cabíveis e a coordenação de treinamentos periódicos e processos de conscientização que se fizerem necessários, podendo, para tanto, contar com a colaboração de equipes externas, desde que estas sejam formalmente aprovadas e contratadas para este fim.

A implantação de novos sistemas operacionais e/ou softwares deve ser informada ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO, para que analise e recomende as alterações da presente Política.

6. **CLASSIFICAÇÃO DAS INFORMAÇÕES**

O Comitê de Segurança é o responsável por estabelecer critérios para classificação das informações, definindo simbologia que permita uma fácil identificação dos documentos classificados, podendo ser uma marca, nota no rodapé ou cabeçalho.

O proprietário da informação deve classificá-la utilizando os modelos padronizados pelo Fórum de Segurança.

A informação deve ser classificada para receber o devido tratamento. Os níveis de classificação das informações são:

6.1. Públicas ou de uso irrestrito – as informações e os sistemas assim classificados podem ser divulgados a qualquer pessoa sem que haja

implicações à instituição. Exemplos: serviços de informação ao público em geral e informações divulgadas pela imprensa ou pela Internet.

6.2. Internas ou de uso interno – as informações e os sistemas assim classificados são restritos ao âmbito da instituição. Caso ocorra divulgação externa das mesmas, as consequências não serão críticas. Exemplos: serviços de informação interna ou documentos de trabalho corriqueiro que só interessam aos funcionários.

6.3. Confidenciais – as informações e os sistemas assim classificados são restritos à instituição e protegidos contra acesso interno e externo não autorizado. O acesso a esses sistemas de informações apenas será feito em caso de estrita necessidade, isto é, usuários podem obter acesso somente se for fundamental para o desempenho de suas funções. O acesso não autorizado compromete o funcionamento da instituição, causando dano financeiro ou perda de fatia de mercado para a concorrência. Exemplos: dados pessoais de empresas e funcionários, senhas, informações sobre vulnerabilidade de segurança dos sistemas institucionais, contratos e balanços.

6.4. Secretas – as informações e os sistemas assim classificados são restritos à instituição, onde o acesso interno ou externo de pessoas não autorizadas a esse tipo de informação é extremamente crítico para a instituição. É imprescindível que o número de pessoas autorizadas seja restrito e o controle sobre o uso dessas informações seja total. Exemplos: dados do departamento pessoal, dados estratégicos, novos negócios, planos de trabalho e etc.

7. **TRATAMENTO DA INFORMAÇÃO**

A cópia ou o armazenamento de informação interna deve ser realizado somente pelos usuários e seu uso deve ser restrito a eles.

A cópia ou armazenamento de informação confidencial ou secreta só pode ser realizada pelo proprietário ou pessoa autorizada. O armazenamento de informações confidenciais deve ser feito em área específica e devidamente protegida dentro dos servidores corporativos da SFA DO BRASIL.

O armazenamento de informações secretas deve ser feito utilizando área criptografada dentro dos servidores corporativos da SFA DO BRASIL.

Todo acesso a informações confidenciais e secretas deve ser auditado.

Os papéis que possuam informações confidenciais ou secretas, que não sejam mais de interesse da SFA DO BRASIL, serão triturados, por equipamentos específicos para este fim.

8. PROTEÇÃO DAS INFORMAÇÕES

8.1 UTILIZAÇÃO

- A responsabilidade pela classificação e local de armazenamento é do proprietário da informação.
- As informações de caráter corporativo da SFA DO BRASIL devem ser armazenadas nos servidores de rede. É responsabilidade do usuário fazer a classificação e consultar a administração da rede para o correto armazenamento.
- Informações confidenciais ou secretas não devem ser armazenadas em diretórios públicos ou estações de trabalho do usuário. Consultar a administração da rede para o correto armazenamento.
- Mensagens de correio eletrônico são consideradas correspondências oficiais. Assim sendo, o usuário deve identificar-se mediante inserção de informações ao final do texto, contendo identificação do remetente e seu cargo ou departamento.
- Cabe ao proprietário, ou detentor de informações confidenciais ou não, a disponibilização das mesmas através de compartilhamentos de rede, previamente solicitados a administração da rede.
- Ao usuário, é expressamente proibido:
    - A transmissão ou posse de informações que impliquem violação de direitos autorais (pirataria);
    - Utilização de linguagem obscena ou profana, que ameace a integridade física ou intimidade de outra pessoa ou organização;
    - Divulgação de qualquer informação classificada como restrita ou confidencial;
    - Utilização do servidor para armazenamento de informações ou arquivos pessoais.
- Os equipamentos de informática funcionarão somente com softwares regularmente adquiridos ou liberados para uso junto a seus fornecedores ou representantes, ou ainda, aqueles elaborados pelo seu quadro de empregados;
- A instalação de softwares sobre os quais a SFA DO BRASIL não detenha direitos e que vise atender interesse de patrocinadoras ou

empresas com as quais mantenha acordo operacional, deverá ser precedida de contrato e que se preserve a SFA de qualquer ônus decorrente da medida;

- Todas as solicitações de aquisição ou desenvolvimento de software deverão ser analisadas pela área de TI, principalmente quanto à compatibilização com equipamentos, linguagens ou softwares adotados pela SFA DO BRASIL;

- O Administrador de Rede deve verificar periodicamente, por meio de ferramentas utilizadas para a administração do ambiente informatizado, possíveis violações das medidas de segurança aplicadas às informações da SFA DO BRASIL. A SFA DO BRASIL reserva o direito de análise de seu parque computacional sem aviso prévio ou comunicado;

- Caso confirmado algum tipo de violação interna às medidas de segurança aplicadas às informações, o Administrador de Rede deve efetuar o bloqueio do acesso do usuário à rede e comunicar o fato ocorrido, imediatamente, ao Gerente da área a que pertence o usuário;

- Todo e qualquer teste, deve ser executado em um ambiente controlado específico para este fim.

- Programas em produção devem estar armazenados fisicamente em local diferente dos programas em desenvolvimento e/ou testes e devidamente protegidos contra acesso não autorizado;

8.2 BACKUP E RESTAURAÇÃO

- A Administração da Rede é responsável por efetuar as operações de Backup e Restauração das informações armazenadas nos servidores da rede corporativa da SFA DO BRASIL;

- Não será realizada cópia de segurança de nenhuma informação ou arquivo armazenado nas estações de trabalho. Esta tarefa é de responsabilidade do usuário.

- Quando necessário, o proprietário da Informação deve solicitar formalmente a Administração da Rede a restauração da cópia de segurança de mensagens do correio eletrônico e arquivos armazenados nos Servidores. Lembrando aos usuários que estas cópias estarão disponíveis conforme a Política de Backup da SFA DO BRASIL;

- O tempo de retenção das mídias será estabelecido de acordo com a Política de Backup adotada pela SFA DO BRASIL;

- Será sempre mantida cópia de segurança acomodado em cofre apropriado para acondicionamento das mídias.

- Será sempre mantida cópia de segurança em localidade externa ao local de localização da infraestrutura;

9. PROCEDIMENTOS DE USO DA REDE INTERNA, HARDWARES E SOFTWARES

A utilização da Infraestrutura tecnológica é fundamental para o desenvolvimento das atividades profissionais pelas quais os usuários da SFA DO BRASIL foram contratados, sendo disponibilizada exclusivamente como ferramenta de trabalho. Com isso, alguns procedimentos devem ser adotados para delinear o que é permitido ou não, bem como garantir o adequado desempenho dessas atividades.

Assim, toda a rede interna, hardwares e softwares estão sujeitos à monitoração e, portanto, a SFA DO BRASIL poderá manter, a seu critério, um histórico de acessos realizados a sua infraestrutura.

Para que esses procedimentos sejam adotados, é importante entender que os termos rede interna, hardware e software se referem a todos os equipamentos de propriedade da SFA DO BRASIL, tais como, mas não se limitando a: computadores desktop, notebooks, softwares homologados, cabos de rede, backbones, equipamentos de discagem (modems), equipamentos de roteamento (roteadores), equipamentos de distribuição (switches e hubs), servidores, firewalls, proxies, impressoras, scanners, smartphones ou qualquer outro equipamento pertencente à infraestrutura tecnológica da SFA DO BRASIL.

Sendo assim, e a partir desse entendimento, seguem as regras:

9.1 USUÁRIOS (CONTAS DE REDE)

Todos os logins de acesso e suas respectivas senhas são pessoais, intransferíveis e de uso exclusivo dos usuários, que assumem integral responsabilidade pela guarda e sigilo de sua senha pessoal, bem como, pelo uso indevido por terceiros, sendo responsável o usuário pela sua disponibilização indevida. Além de tais cuidados, o usuário não deve utilizar sua conta, ou qualquer outra conta, para violar ou transpor as definições contidas nesta Política.

Caso qualquer vulnerabilidade do sistema operacional seja constatada por usuário da SFA DO BRASIL, este, imediatamente, deverá informar ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO sobre tal vulnerabilidade, sendo que qualquer utilização ilícita da infraestrutura tecnológica da SFA DO BRASIL seja pelo aproveitamento de falhas de segurança, ou pela

simples tentativa de erro ou de acerto de senhas, o sujeitará às devidas sanções.

Para tanto, seguem as normas definidas:

a) Não é permitido compartilhar a conta de usuário e senha com outro usuário e/ou terceiro;

b) Não é permitida nenhuma tentativa e/ou acesso de outras contas de usuário que não a sua pessoal;

c) Não é permitida nenhuma tentativa e/ou acesso para transpor a autenticação ou segurança do computador, rede ou conta;

d) Não é permitida nenhuma tentativa e/ou interferência com serviços da rede, das máquinas e outros dispositivos.

O RH deve informar à infraestrutura, sempre que houver desligamento, no prazo de 24 (vinte e quatro) horas, a relação de usuários desligados, ou em processo de desligamento para que os acessos sejam imediatamente bloqueados pelo Administrador da Rede.

9.2 PROCEDIMENTO IDENTIFICAÇÃO DO USUÁRIO

O cadastro de colaborador no Ambiente de TI será solicitado, imediatamente após sua admissão, pela área interessada ao departamento de Recursos Humanos e esta à Gestão de TI Corporativa via formulário padrão.

O cadastro de terceiros para acesso aos recursos da rede e sistemas deve ser efetuado mediante requisição da área interessada a Gestão de TI Corporativa, via formulário padrão, ou através de contrato de prestação de serviço;

Todo cadastro solicitado deverá ser arquivado para formação de registro histórico das operações;

O desligamento do colaborador será notificado imediatamente pelo Departamento RH a Gestão de TI Corporativa via chamado / solicitação ao sistema interno que tomará as providências necessárias para o cancelamento da login bem como para proceder a devolução, se houver, dos equipamentos da SFA DO BRASIL por ele utilizados.

A criação e manutenção do login de identificação do usuário na rede e sistemas devem seguir as seguintes regras:

Será utilizado o NOME.SOBRENOME do usuário Exemplo:

Nome Usuário 1: João Antonio Cabral

Nome Usuário 2: Marco Aurelio Silva Santos

Nome Conta de acesso 1 (E-mail, Sistemas, Rede, etc): joao.cabral

Endereço de E-mail: joao.cabral@sfadobrasil.com.br

Nome Conta de acesso 2 (E-mail, Sistemas, Rede, etc): marco.santos

Endereço de E-mail: marco.santos@sfadobrasil.com.br

Em caso de duplicidade de logins será considerado o nome anterior ao sobrenome até que a duplicidade seja desfeita;

Sobrenomes terminados em: Filho, Neto, Sobrinho prevalece a regra acima de retroceder ao nome anterior ao sobrenome.

Ex. Nome Usuário 1: Paulo Henrique da Silva Filho

Nome Usuário 2: Joao Pereira Abravanel Neto

Nome Conta de acesso 1 (E-mail, Sistemas, Rede, etc): Paulo.silva

Endereço de E-mail: paulo.silva@sfadobrasil.com.br

Nome Conta de acesso 2 (E-mail, Sistemas, Rede, etc): Joao.abravanel

Endereço de E-mail: joao.abravanel@sfadobrasil.com.br

O usuário terá a mesma identificação para todos os ambientes que a requererem;

9.3 SENHAS

Toda conta de usuário tem sua respectiva senha que provê acesso aos recursos autorizados a cada usuário da SFA DO BRASIL, de acordo com seu perfil, que deverá mantê-la em segurança.

As solicitações de criação, exclusão e alteração de usuários deverão ser feitas através do formulário padrão, definido pelo COMITÊ DE SEGURANÇA DA INFORMAÇÃO, e encaminhadas ao RH, por e-mail à área de Infraestrutura que cadastrará o usuário de acordo com suas permissões para dentro dos sistemas. A senha inicial será padrão, que

deverá ser alterada de acordo com as políticas em vigor. A área de Infraestrutura será a única responsável pela concessão de acessos e somente atenderá tais solicitações.

a) Todos os campos do formulário devem estar preenchidos com informações fidedignas;

b) As solicitações devem ser provenientes de usuários que tenham autorização para efetuar tal solicitação em razão de seu nível hierárquico, normalmente solicitação do RH;

c) o usuário ou líder direto receberá em seu e-mail os dados de conta e sistema para acesso, bem como a senha inicial padrão que deverá ser alterada;

O uso indevido de senhas poderá gerar responsabilidades civis e criminais, conforme dispõe o art. 325 do Código Penal: Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:

A conta do usuário será suspensa em situações de afastamento do trabalho ou demissão. O líder ao qual o usuário afastado pertence, deverá comunicar sobre o afastamento e solicitar a suspensão da senha à área de RH, que, por sua vez, encaminhará a comunicação e a solicitação à área de infraestrutura.

Os usuários devem obrigatoriamente escolher senhas difíceis de serem decifradas. Isso significa que não devem ser utilizadas senhas que possam ser relacionadas ao trabalho ou a vida pessoal.

Além da necessidade de possuir no mínimo 8 caracteres, a senha deve respeitar no mínimo 3 dos 4 critérios abaixo:

Um ou mais caracteres minúsculos;

Deve-se utilizar mínimo de uma letra maiúscula (A, B, C, D, ...Y,Z).

Pelo menos (1) um caractere numérico.

Pelo menos (1)um caractere especial (!, @, #, $, %, %, &, ,*)

Além disso, a senha NÃO poderá:

Constar o próprio login ou dados do cadastro pessoal na composição da senha.

Não utilizar as últimas 4 senhas.

Os usuários podem escolher senhas de fácil memorização e ao mesmo tempo de difícil adivinhação como, por exemplo: Usando iniciais de um conjunto de palavras.

As senhas resultantes deste processo são conhecidas como pass phrases

9.4. TROCA DE SENHAS

As senhas devem ser trocadas no Máximo a cada 90 (noventa) dias. O Comitê de Segurança pode solicitar a troca das senhas de forma parcial ou total na organização sem prévio aviso.

9.5. BLOQUEIO DA CONTA

Como forma de garantir a segurança, a conta será automaticamente bloqueada após 5 tentativas com a senha diferente da cadastrada no banco de dados. O prazo de bloqueio da conta é de 2 horas. Havendo a necessidade ativar imediatamente o usuário deve ligar para o administrador da rede para troca ou através do portal de serviços da Gestão de TI Corporativa.

9.6. HISTÓRICO DE SENHAS

Para impossibilitar a utilização de senhas repetidas pelos usuários, os aplicativos devem manter um histórico das 4 últimas senhas utilizadas. Para aqueles aplicativos que não possuem esta funcionalidade, a utilização de senhas com números maiores de caracteres deve ser considerada.

10. USO E CONTROLE DE INFORMAÇÕES, DADOS E ARQUIVOS

10.1. ARQUIVOS COMUNS

Todos os documentos eletrônicos, dados e informações da atividade laborativa dos usuários devem estar bem protegidos, no diretório específico para cada usuário, destinado a arquivos de trabalho. A Infraestrutura da SFA DO BRASIL irá dispor de um servidor de arquivos e garantirá, através dele, o sigilo das informações, bem como, o backup dos mesmos, a fim de garantir sua integridade.

O uso da capacidade de armazenagem de dados no servidor deve ser feito com tolerância, no sentido de armazenar arquivos sem duplicações, salvo quando estas forem exigidas. Não é permitida a utilização do servidor para armazenar dados e ativos pessoais dos usuários, assim entendidos como aqueles que não são de interesse, uso ou propriedade da SFA DO BRASIL.

Os usuários, excetuando-se os que tenham autorização específica para esse fim em razão de seu perfil, não podem permitir ou causar qualquer alteração, bem como, destruição de sistemas operacionais, dados ou comunicações de propriedade da SFA DO BRASIL.

As informações, independentes da classificação e criticidade que estiverem armazenas nas estações de trabalho são de responsabilidade do usuário. Havendo a necessidade pelo Backup o mesmo deve solicitar a Gestão de TI o formulário para correto entendimento e preenchimento quanto a forma de backup.

10.2. E-MAIL

Todas as mensagens trafegadas possuem uma cópia retida junto ao servidor, com a finalidade de realizar auditoria, quando necessário. Portanto, é extremamente importante que o usuário não coloque em risco informações da SFA DO BRASIL ao enviar email para alguns destinatários. Também fica proibida a comunicação excessiva através de e-mail para tratar assuntos particulares, sejam eles com pessoas da SFA DO BRASIL ou fora dela. O Usuário não tem privacidade sobre o conteúdo, portanto pode sofrer sanções sérias quando infringir o Código de Ética e Conduta de Negócios e Política Anticorrupção da SFA DO BRASIL.

Apesar de o Correio Eletrônico estar protegido por sistema antivírus, fica vedada a INSERÇÃO ou DISSEMINAÇÃO de arquivos que contenham vírus ou qualquer espécie de programas nocivos, sob pena de responsabilização do usuário.

Não será permitido o envio de qualquer informação corporativa da SFA DO BRASIL ou de seus parceiros, seja esta revestida de sigilo ou não, fornecedores, clientes e terceiros;

Não será permitido o envio de quaisquer arquivos que violem direitos de terceiros, ou que possam causar prejuízos, a terceiros e/ou da SFA DO BRASIL;

Não será permitido o envio de qualquer arquivo com conteúdo que configure prática de infração penal ou ilícito civil em face da SFA DO BRASIL e/ou de terceiros;

Não será permitida a prática de qualquer ato que configure concorrência desleal ou quebra de sigilo profissional;

Não será permitido o envio de qualquer arquivo de caráter ilegal, ofensivo e/ou imoral, de forma genérica.

10.3. MENSAGEM INSTANTÂNEA

A SFA DO BRASIL permite aos USUÁRIOS, a utilização de uma ferramenta para envio de mensagens rápidas, buscando evitar a utilização do telefone e agilizar a comunicação para algumas áreas da empresa.

10.4. SOFTWARES

A SFA DO BRASIL disponibiliza para seus usuários um conjunto de softwares exclusivamente para o desempenho de suas atividades profissionais, assim, é vedada a utilização de quaisquer softwares não homologados pela infraestrutura da empresa.

Dessa forma, os usuários somente poderão instalar programas que sejam autorizados e homologados pela Infraestrutura da SFA DO BRASIL. Fica, portanto, vedado ao usuário a instalação de qualquer software, inclusive softwares de avaliação (trial), open source e gratuito, sem autorização prévia e expressa da infraestrutura retro citada, excetuando-se aquele usuário que tem permissão expressa em razão de seu cargo, mas devendo seguir as políticas de software da empresa.

Todos os softwares instalados nos computadores da SFA DO BRASIL são devidamente licenciados ou de conhecimento do Comitê de Segurança, e o uso de qualquer software que não seja autorizado e/ou que viole os direitos do autor do programa de computador, são terminantemente proibidos. O desrespeito a essas normas caracteriza infração à lei e ao contrato, gerando encargo exclusivo do usuário que arcará com a responsabilidade criminal, trabalhista e civil.

Portanto, os usuários ficam cientes da obrigação de indenizar da SFA DO BRASIL caso esta venha a suportar qualquer prejuízo em demandas judiciais ou administrativas movidas pelos titulares dos direitos autorais de tais programas não autorizados, bem como, de qualquer outra obra intelectual violada em seus direitos autorais, incluindo as despesas com custas e honorários advocatícios, bem como os efeitos do artigo 70, inciso III, do Código de Processo Civil (denunciação da lide), concordando com a sua inclusão no polo passivo da demanda.

Softwares que atendem individualmente ao usuário como agendas, editores de imagem, vídeo, visualizadores, gestão financeira entre outros softwares específicos mesmo que na modalidade open, trial, free devem passar pela área de Gestão de TI antes da sua instalação.

10.5. HARDWARES

A SFA DO BRASIL disponibiliza para seus usuários um conjunto de equipamentos e máquinas exclusivamente para o desempenho de suas atividades profissionais, assim, o uso inadequado desses equipamentos e para fins que não sejam os delineados pela empresa, é proibido.

É vedado o uso de quaisquer equipamentos que não sejam de propriedade da SFA DO BRASIL para conexão em sua rede corporativa, especialmente os notebooks e smartphones particulares, já que comprometem a Segurança da Informação e também qualidade dos serviços.

É vedado o uso de quaisquer equipamentos que não sejam de propriedade da SFA DO BRASIL para conexão em sua rede corporativa, especialmente os notebooks e smartphones particulares, já que comprometem a Segurança da Informação e também qualidade dos serviços.

Na utilização de todos os hardwares e periféricos de propriedade da SFA DO BRASIL, o usuário deverá observar os seguintes cuidados:

a) Desligar o equipamento no final do expediente, ou em ausências prolongadas;

b) Toda vez que não for mais utilizar o computador, ou for se ausentar da sala, efetuar o bloqueio da rede, evitando que terceiros usem o nome de usuário ilicitamente;

c) Sempre que tiver dúvidas ou problemas nos equipamentos, contatar a área de infraestrutura, pelo e-mail: suporte@sfadobrasil.com.br

A alteração de qualquer periférico ou componente nos computadores não é permitida, ficando vedada aos usuários. A realização de qualquer modificação ou manutenção deverá sempre ser realizada pela área de TI.

Em casos de desligamento os usuários que possuírem equipamentos móveis deverão deixá-los com a TI que realizará o processo de restauração das configurações de fábrica do aparelho, eliminando assim, os dados da SFA DO BRASIL. Estes dispositivos não se limitam a notebooks, etc (particulares ou não). A responsabilidade de comunicar a TI deve ser do líder do processo ou gestor da área. Caso o comunicado não ocorra a TI se isenta de problemas eminentes.

10.6. EQUIPAMENTOS PORTÁTEIS

Por se tratar de equipamentos portáteis nos quais informações da SFA DO BRASIL estão armazenadas, o usuário não deve deixar esses equipamentos fora do seu alcance em locais públicos, onde haja acesso de múltiplas pessoas, bem como, não deve permitir que terceiros não autorizados tenham acesso às informações ou dados transportados nesses equipamentos, empregando todos os cuidados necessários para que não haja vazamento de informações.

Os equipamentos portáteis, tais como, mas não se limitando a: notebooks, smartphones, pendrive e quaisquer outros que permitam armazenamento de dados e informações somente poderão ser utilizados pelos usuários dentro da estrutura (dentro da empresa) se disponibilizados da SFA DO BRASIL ou em comum acordo com a SFA DO BRASIL, a seu exclusivo critério. Desse modo, é expressamente vedada a utilização de equipamentos portáteis particulares para o desenvolvimento das atividades profissionais relacionadas a SFA DO BRASIL, sem expressa autorização desta, bem como a cópia e/ou transferência de informações ou dados de propriedade da mesma através destes equipamentos.

Os notebooks da SFA DO BRASIL que por ventura forem para a casa do usuário por qualquer situação pertinente ao trabalho, devem voltar à empresa íntegros, sem softwares adicionais inclusos. Caso o equipamento tenha ficado exposto a situações de risco com vírus, antes de ligar dentro da infraestrutura da SFA DO BRASIL, o mesmo deve ser entregue à equipe de TI para que esta tome as medidas de prevenção adequadas.

Este procedimento vale também para notebooks particulares que foram adquiridos com o auxílio da SFA DO BRASIL e, portanto, são instrumentos pertinentes a execução do trabalho. A única exigência é que este equipamento deve seguir as mesmas políticas de computadores da , inclusive ter instalado softwares de monitoramento de irregularidades.

10.7. IMPRESSORAS

O uso das impressoras deve ser feito exclusivamente para impressão de documentos ou outras informações que sejam de interesse da SFA DO BRASIL ou que estejam relacionados com o desempenho das atividades pelas quais os usuários foram contratados.

Impressões que contenham informações sensíveis que não tenham mais utilidade devem ser destruídas, visando preservar o sigilo. A SFA DO BRASIL, em cumprimento ao seu compromisso com a responsabilidade social, recomenda que sejam impressos apenas documentos indispensáveis, devendo os demais ser lidos na própria tela do computador ou arquivados em forma de arquivo virtual.

10.8. CONTROLE E GERENCIAMENTO DE ANTIVÍRUS

Sem prejuízo do controle automático dos servidores da SFA DO BRASIL, todos os usuários são responsáveis também pelo controle de dados que possam estar infectados. Quando detectada uma mensagem ou anexo contaminados por código malicioso, esta mensagem e seus anexos serão eliminados.

Os usuários também são responsáveis pela não interrupção da verificação periódica das suas estações de trabalho, bem como, de qualquer dispositivo portátil que possa conter arquivos, antes de acessá-lo. Em quaisquer situações, todo e qualquer arquivo proveniente de redes ou usuários externos deverão, obrigatoriamente, ser verificados por sistemas de proteção contra vírus.

10.9. ACESSO REMOTO VIA VPN (VIRTUAL PRIVATE NETWORK)

A concessão de acesso remoto e via VPN será a exclusivo critério da SFA DO BRASIL, que optará por qual rede o usuário terá permissão de acesso. Referida concessão será feita de forma individual, sendo os usuários responsáveis por seus acessos via VPN, bem como, por qualquer atividade irregular exercida por outra pessoa de posse de seu acesso remoto. Com isso, os usuários deverão adotar medidas de cautela, para que terceiros não tenham acesso, sem autorização, à sua porta VPN.

10.10. USO DE REDES EXTERNAS (INTERNET E OUTRAS)

O acesso a redes externas, principalmente a Internet, é fundamental para o desempenho de algumas atividades relacionadas ao trabalho, assim, o uso da Internet deve estar voltado para o acesso às informações relacionadas somente com as atividades de interesse da empresa. Os acessos originados na rede interna da empresa com destino a qualquer rede externa, só podem ser realizados através dos equipamentos da SFA DO BRASIL destinados a realizar o roteamento das redes, bem como, devem ser feitos com a utilização de firewall e proxy de acordo com as regras de navegação e acesso abaixo definidas.

A navegação a sites não relacionados diretamente à atividade laborativa do usuário, não é proibida, porém, seu uso deve ser feito de maneira equilibrada e responsável, antes do início do expediente ou no horário de almoço, para assegurar ao usuário e à empresa máxima segurança e performance no trabalho, de modo que abusos serão punidos.

Excetuam-se desta previsão aqueles sites de categoria restrita pela SFA DO BRASIL, cuja navegação é expressamente proibida. Fica estipulada a seguinte política para acessos à Internet:

a) Da rede interna para a Internet somente poderá ser realizada a navegação através de acesso autenticado;

b) Fica terminantemente proibida a navegação aos sites pertencentes as categorias e atividades que exponham a SFA DO BRASIL e suas informações sensíveis, conforme classificação abaixo;

Casos Leves

- Jogos;
- Sites de relacionamento (Facebook, Twitter e demais do gênero);
- Instant messenger (MSN, Skype e demais do gênero);
- Propaganda Político Partidária;
- Áudio e Vídeo (Acesso ou Compartilhamento (ex: peer to peer)) salvo com conteúdo relacionado diretamente a SFA DO BRASIL;
- Violação de direito autoral (pirataria, etc);
- Conteúdo impróprio, ofensivo, ilegal, discriminatório e similares;
- Webmail Particular (Ex: Gmail, Hotmail, Uol, Terra, Globo e etc);
- Transferência de arquivos de programa a partir da internet sem autorização prévia dos administradores da rede interna;

Casos Médios

- Pornográfico e de caráter sexual;
- Crackers;
- Ferramentas de Proxy;
- Violência e Agressividade (racismo, preconceito e conteúdos similares)

Casos graves

- Acesso externo com a finalidade de divulgação de dados sigilosos/sensíveis (Ex: Planejamento Estratégico, Propostas Comerciais, Informações financeiras, e dados correlatos a atividade da empresa sem prévia autorização);
- Acesso a conteúdo sobre “Terrorismo” e disseminação de violência a partir de crença ou posição política;
- Utilização de acesso interno para práticas de comercialização, divulgação ou posicionamento sobre Drogas, alucinógenos ou substâncias entorpecentes;
- Pornografia Infantil (pedofilia);

Observação: É permitido o uso do Skype para tratar de assuntos relacionados ao trabalho executado.

c) A transferência de arquivos via FTP, quando imprescindível, será autenticada;

d) Dispositivos de controle e segurança deverão ser utilizados, para garantir a confidencialidade e a integridade das informações em tráfego por estas redes;

e) É proibido acessar todo e qualquer site que apresente vulnerabilidade de segurança ou que possa comprometer, de alguma forma, a segurança e a integridade da rede da SFA DO BRASIL. As conexões deverão ocorrer exclusivamente através de acesso autenticado;

f) O Acesso a Rede de Visitantes (denominada “REDEGUEST”), será liberado somente para fins de acesso à internet, via sistema de voucher (com duração máxima de 12 horas), a partir da solicitação e aprovação do administrador de rede/gerente de infraestrutura. As regras de acesso e penalidades serão as mesmas listada na alínea “b”, logicamente considerando a penalidades passíveis de aplicação aos usuários visitantes.

10.11. GUARDA DE LOGS E AUDITORIA

Todas as atividades desenvolvidas com a utilização da infraestrutura tecnológica da SFA DO BRASIL serão registradas para eventual fim judicial, além de análise ou auditoria, por um período de 03 (três) meses. Essas atividades incluem acesso à rede, informações, logs de envio e recebimento de mensagens eletrônicas, acesso e navegação a sites, uso dos aplicativos e softwares das estações de trabalho e outros. Mensalmente será realizada auditoria interna por um responsável da Infraestrutura da SFA DO BRASIL.

O processo de auditoria das estações de trabalho, servidores e outros devem acontecer periodicamente sem aviso. A Gestão de TI poderá aplicar a auditoria sempre que julgar necessário ou quando solicitado pela diretoria da empresa.

Estão inclusos na auditoria a seguintes ações:

- Auditoria parcial ou total as estações de trabalho;
- Auditoria as caixas de correio eletrônico;
- Auditoria aos logs de internet e demais sistemas da companhia.

10.12. CÂMERAS DE FILMAGEM

A fará uso de câmeras de segurança instaladas em suas dependências, ficando resguardada a dignidade humana dos usuários, sendo vedada a instalação de câmeras de filmagem nos banheiros e lavabos.

A filmagem descrita nesta Política tem por objetivo verificar o respeito dos usuários às regras estabelecidas no presente instrumento, bem como, assegurar segurança física aos mesmos, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa filmada, com o que os usuários declaram, expressamente, neste ato, concordar.

As imagens captadas dentro das dependências da SFA DO BRASIL serão arquivadas pelo prazo de 60 (sessenta dias e mantidas em caráter estritamente confidencial, somente podendo ser divulgadas em caso de infração às regras constantes da presente Política e/ou infração de legislação vigente.

11. RESPEITO AS NORMAS E POLÍTICAS VIGENTES

A SFA DO BRASIL possui normas e políticas que são periodicamente revisadas e tem valor legal através deste documento. Entre as Normas e Políticas, temos: Política de Senhas; Norma de Utilização do Correio Eletrônico; Política de Backup; O USUÁRIO da SFA DO BRASIL tem por obrigação cumprir todas as políticas publicadas e o não cumprimento será considerado um incidente e poderá sofrer sanções previstas.

12. SANÇÕES

O USUÁRIO tem por obrigação cumprir todas as políticas publicadas e o não cumprimento será considerado um incidente. Por meio do Comitê de Segurança, da SFA DO BRASIL exercerá seu poder perante o conhecimento desta Política para aplicar sanções aos infratores do mesmo. Inicialmente o incidente será classificado em 3 níveis:

Casos Leves: quando não há risco ao bom nome da empresa ou exposição de informações classificadas como sensíveis. Um exemplo de caso leve é o uso eventual de recursos particulares, como acessos a websites fora do contexto das atividades da empresa, compras e webmail particular.

Casos Médios: Reincidências de casos leves ou casos incidentes onde seja comprovada a não intenção de dolo.

Casos Graves: Quando a ação ou omissão do usuário exponha ou cause danos a informações classificadas como sensíveis e atos que denigram a imagem da SFA DO BRASIL. Tentativas deliberadas de acesso, não expressamente autorizado, a dados sensíveis constituem claramente um caso grave. Atividades ilícitas vinculadas as atividades de “Terrorismo”, “Pedofilia” e comercialização de “Drogas” são automaticamente consideradas como Casos Graves.

12.1 SANÇÕES PARA O USUÁRIO (FUNCIONÁRIO)

Na constatação de um incidente (previamente classificado), as seguintes sanções serão aplicadas;

Advertência Verbal: Aplicada na constatação de incidente categorizado como Caso Leve. Esta advertência será comunicada diretamente ao USUÁRIO (Funcionário), pelo Comitê de Segurança da Informação.

Advertência Escrita: Será avaliada pelo Comitê de Segurança da Informação, informado ao Departamento de RH para aplicação desta advertência conforme legislação pertinente (CLT – Consolidação das Leis de Trabalho).

Demissão: Será aplicada de acordo com a legislação pertinente (CLT – Consolidação das Leis do Trabalho). Não existe uma ordem para a aplicação das sanções, sendo assim, um incidente pode ter punição máxima sem que tenha havido qualquer outro incidente anterior.

12.2 SANÇÕES PARA O USUÁRIO (PRESTADOR DE SERVIÇO)

Na constatação de um incidente (previamente classificado), o COMITÊ DE SEGURANÇA irá avaliar e aplicará as medidas cabíveis conforme o contrato de prestação de serviço.

13. VALIDADE DA POLÍTICA

A presente Política Interna de Segurança da Informação tem o início da sua validade com o Aceite dos Gestores da SFA DO BRASIL e sua publicação no site d empresa no endereço https://sfadobrasil.com.br. Seu prazo de validade é indeterminado, podendo somente sofrer modificações no seu conteúdo sem aviso prévio.

14. APLICAÇÃO DA POLÍTICA

A presente Política Interna de Segurança da Informação poderá ser aplicada após a retenção da assinatura do usuário sobre o conhecimento e concordância de todos os termos deste documento.

14.1 PARA OS USUÁRIOS JÁ EXISTENTES

Quem já possui vínculo com a , ficará exposta esta Política em meios de acesso a todos, onde terão um prazo para ler e aceitar as regras que entrarão em vigência. Logo após este deverá ir até a área de Gestão de Pessoal e Contratos assinar o Termo de Comprometimento com a Segurança da Informação. Caso o usuário se negue a assinar, será convidado a um encontro com o Comitê de Segurança que tentará dar um significado para a importância para a que todos trabalhem de acordo com esta regulação.

14.2 PARA NOVOS USUÁRIOS

Este documento deverá ser entregue no momento da contratação, que só poderá ser efetuada mediante a coleta da assinatura de aceite no Termo de Responsabilidade da Segurança da Informação.

Contamos com sua colaboração!

SFA DO BRASIL

Termo de Política Interna de Segurança

Eu, _____ declaro estar ciente que a SFA DO BRASIL SERVIÇOS DE INFORMÁTICA LTDA, adota uma Política Interna de Segurança da Informação. A esse respeito, afirmo ter recebido a Política, e que, depois de lê-la, aceito-a na sua íntegra, comprometendo-me ao cumprimento de todas as suas disposições, ficando sujeito(a) às sanções previstas em consequência de alguma transgressão ou descumprimento.

Data:_____/_____/_____

Assinatura: _____