



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

FUSÃO

Sumário

OBJETIVO: 3

DOMÍNIO DE APLICAÇÃO: 3

INSTRUÇÕES: 3

1. Organização Geral: 3
2. Normas e Respeito à propriedade intelectual: 4
3. Contas de Acessos e Senhas: 4
4. Utilização do Correio Eletrônico: 6
5. Utilização da Internet: 7
6. Proteção dos dados e Sistema de Informação: 8
7. Utilização de Compartilhamentos e Grupos de Trabalho: 9
8. Engenharia Social: 10
9. Conclusões: 10

Recibo de Entrega DA POLÍTICA DE Segurança da Informação da FUSÃO

11

OBJETIVO:

O presente documento tem por objetivo dar conhecimento e estabelecer níveis de responsabilidade quanto ao uso e posse dos recursos informáticos (equipamentos e softwares), meios de comunicação eletrônicos e demais informações, sob a forma digital ou física, necessários ao desempenho das atividades profissionais, durante a vigência do contrato de trabalho, serviço ou estágio.

DOMÍNIO DE APLICAÇÃO:

Esta instrução se aplica aos funcionários, prestadores de serviços, consultores, auditores, fiscais, temporários e demais colaboradores que estejam a serviço das empresas que fazem parte da FUSÃO, incluindo toda a mão-de-obra terceirizada ou disponibilizada mediante convênios, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas. Abrange todos os sistemas e equipamentos de propriedade da FUSÃO, bem como aqueles de propriedade de terceiros que lhes sejam confiados a qualquer título ou cedidos pela mesma a terceiros.

INSTRUÇÕES:

1. Organização Geral:

Os recursos informáticos, tais como equipamentos (notebook, desktop, iPad, rede Wi-Fi, 3G, telefone fixo e móvel etc.), programas (Word, Excel, Project, etc.), sistemas (VM SYSTEM, TRON, ALTERDATA, etc.) e informações da Fusão, são colocados à disposição de todos aqueles abrangidos por esta Política, para fins exclusivamente profissionais e devem ser utilizados apenas para o cumprimento da atividade profissional, não sendo permitido seu uso para quaisquer outros fins (de diversão, econômicos particulares, políticos, religiosos, pedófilos, sexuais e demais) que possam responsabilizar civil ou penalmente a Fusão.

Não é permitido acessar os sistemas da Fusão para os quais o usuário não possui direito de acesso, tampouco tentar acessar contas de outros colaboradores ou apropriar-se de seus direitos de uso, seja qual for o meio. Qualquer anormalidade deve ser imediatamente reportada ao Gestor imediato.

Apenas os equipamentos autorizados pelo Departamento de TI (tais como: Notebook Fusão, Smartphone Fusão, Pendrive Fusão, etc.) podem ser conectados à rede da Fusão. A conexão de outros equipamentos (como câmeras / filmadoras, iPads pessoais não autorizados, i-Pods, HDs externos, Pendrives pessoais, etc.) pode representar riscos para a organização e, portanto, depende inicialmente da aprovação pelo Gestor imediato e de uma aprovação prévia do Departamento de TI da Fusão.

2. Normas e Respeito à propriedade intelectual:

Por razões de segurança de funcionamento e de direitos de licença, somente os softwares autorizados pela Fusão poderão ser utilizados ou instalados nos equipamentos da empresa.

Todos os aplicativos, softwares, dados e informações protegidas por direitos de autoria ou direitos de propriedade intelectual de terceiros (Nero, Adobe, Skype, etc.), somente podem ser utilizados após autorização dos titulares dos direitos, por meio de licenças formais e aprovação do Departamento de TI.

Não é permitida a instalação de protetores de tela, papel de parede, temas para a área de trabalho ou similares, sendo autorizado utilizar apenas padrões estabelecidos pela empresa.

3. Contas de Acessos e Senhas:

Todos os colaboradores receberão uma Conta de Identificação Pessoal – LOGIN de acesso aos Sistemas de Informação da Fusão e esta conta permitirá o seu acesso aos ambientes necessários para o cumprimento das suas atribuições funcionais.

As senhas para acesso por meio da Conta de Identificação Pessoal são de uso EXCLUSIVO do colaborador, salvo autorização formal e expressa do seu Gestor imediato. O Colaborador possui inteira responsabilidade por todas as transações realizadas com a sua conta de acesso, haja vista que são de uso pessoal e intransferível.

A partir da confirmação da criação de qualquer conta de acesso, o usuário tem um prazo máximo de setenta e duas (72) horas úteis para a primeira conexão e testes das funcionalidades.

O usuário deve trocar a senha padrão no primeiro acesso e se comprometer a seguir os critérios definidos para a criação de senhas consistentes (não óbvias).

O usuário deve atender às solicitações periódicas de troca de senhas e se comprometer a seguir os critérios definidos para a criação de senhas consistentes (não óbvias).

Caso seja constatada a inatividade das contas de acessos (falta de conexão ou uso) por mais de 40 (quarenta) dias consecutivos, a Fusão suspenderá o acesso do usuário aos ambientes, como medida de proteção.

Caso seja constatada a inatividade das contas de acessos (falta de conexão ou uso) por mais de 90 (noventa) dias consecutivos, o usuário deve entrar em contato com o Departamento de TI para regularizar a situação. Caso contrário, a Fusão excluirá totalmente o acesso aos ambientes como medida de proteção dos seus ativos, o que impedirá o usuário de ter acesso aos sistemas e aplicativos corporativos.

Em casos de roubos ou perdas dos recursos móveis (notebook, iPad, telefone celular, etc.) ou dos meios de acessos a esses recursos (smartcard, senhas, chaves VPN, etc.), o usuário deve comunicar imediatamente às autoridades policiais, bem como ao Gestor imediato e ao Departamento de TI da Fusão.

O usuário deve informar previamente ao seu gestor imediato, bem como ao RH da Fusão a ausência (licença médica, formação, licença sem vencimento etc.) que possa causar a INATIVIDADE da sua conta de e-mail ou login de acesso ao sistema (falta de uso ou de conexão) superior ao prazo de

30 (trinta) dias, como medida de proteção às suas atribuições e acessos, sendo de responsabilidade do Gestor imediata do usuário e do RH a respectiva comunicação ao Departamento de TI.

Será de responsabilidade do RH da Fusão, a comunicação prévia ao Departamento de TI sobre possíveis mudanças de postos que porventura tenham como consequência mudanças no perfil de acesso de cada usuário.

Será de responsabilidade do RH da Fusão, a comunicação prévia ao Departamento de TI sobre a admissão (aumento de quadro) com informações de: nome completo, departamento, cargo, necessidade de equipamentos a serem adquiridos e os acessos necessários (e-mail, rede, sistema).

Será de responsabilidade do RH da Fusão, a comunicação prévia ao Departamento de TI sobre a demissão de colaboradores, solicitando o cancelamento dos acessos do usuário com informação exata da data do ocorrido.

4. Utilização do Correio Eletrônico:

Não é permitido criar ou propagar mensagens cujo conteúdo tenha características ofensivas, difamatórias, racistas, tampouco mensagens de natureza política, sexual, pornográfica ou pedófila.

É dever de cada usuário proteger adequadamente arquivos, através do uso da solução própria da Fusão, que contenham informações sensíveis, antes de enviá-los por E-Mail.

O usuário deve assegurar a devida correção dos endereços dos destinatários antes de enviar qualquer e-mail, evitando envolver pessoas não autorizadas em assuntos que não lhes dizem respeito.

O correio eletrônico e o endereço de e-mail que foram disponibilizados aos usuários pela Fusão, devem ser utilizados para assuntos corporativos. Nos casos em que for permitido o uso particular, o usuário se compromete a utilizar os recursos de forma moderada.

Para a segurança do sistema informático da empresa, a Fusão poderá executar periodicamente, ou quando se fizer necessário, verificações no fluxo e

teor das mensagens de cada usuário, a fim de acompanhar o cumprimento das regras existentes nesta Política de Segurança da Informação.

Só é permitido a utilização do sistema de correio eletrônico por interface web, não sendo autorizada a utilização de softwares como Zimbra, Outlook, etc. Exceções poderão ser aplicadas somente mediante autorização prévia do Departamento de TI.

Para o envio dos e-mails, deverão ser utilizados apenas os modelos padrões de formatação, logo e assinaturas estabelecidos pela empresa.

5. Utilização da Internet:

O usuário fica expressamente ciente de que representa a Fusão quando acessa uma rede externa, e se compromete em não participar de contatos e intercâmbios que possam comprometer a imagem e bom nome da Fusão.

Só é permitido acessar chats ou fóruns, cujos participantes são conhecidos, desde que autorizado pela Fusão.

O usuário deve respeitar as restrições de acesso a webmails pessoais / privados, via Internet, que somente poderão ser feitos mediante autorização prévia ou liberalidade expressa da Fusão.

A Fusão restringe e proíbe a execução de downloads, via Internet, de arquivos que não sejam compatíveis com as atividades profissionais (softwares freeware ou shareware, músicas MP3 ou MP4, filmes).

A Fusão restringe e proíbe o acesso a sites de streaming de vídeos e músicas (rádios online, youtube, etc).

Não é permitido conectar sites que contenham informações que possam ser objeto de consequências penais, tanto para o usuário, quanto para a Fusão.

O usuário possui obrigação de estar constantemente informado e atualizado sobre as regras de segurança do site da instituição bancária com a qual trabalha, por entender que a Fusão apenas disponibiliza o meio de comunicação, mas não tem qualquer responsabilidade por problemas com fraudes e invasões realizadas no ambiente da instituição bancária.

É expressamente proibição de criação de páginas pessoais, bem como hyperlinks entre o(s) site(s) da Fusão e outro site qualquer, sem que tenha uma prévia autorização da Fusão para tal.

Os recursos para acesso à Internet e a respectiva conta de acesso, que foram disponibilizados pela Fusão, devem ser utilizados para os assuntos corporativos.

Para a segurança do sistema informático da empresa, poderá a Fusão fazer verificações periódicas ou quando se fizer necessário nos históricos dos acessos de cada usuário, de maneira a comprovar o cumprimento das regras existentes nesta Política de Segurança da Informação.

Obs. Todas as práticas descritas neste item estão condicionadas à liberalidade da Fusão, portanto, caso a Fusão autorize o uso particular o usuário se compromete a utilizar os recursos de forma moderada.

6. Proteção dos dados e Sistema de Informação:

O usuário é o único responsável pelo armazenamento de dados contidos em sua estação de trabalho e os arquivos e pastas criados ou utilizados pelo usuário serão protegidos pelo sistema de backup somente se armazenados nos servidores.

Os recursos informáticos da Fusão devem servir para o armazenamento de dados pertinentes às atividades corporativas ou de informações de interesse da Fusão. Em caso de liberalidade por parte da Fusão, o usuário deve se comprometer em armazenar, de forma moderada, informações particulares.

O transporte, o armazenamento, e o tratamento de informações da Fusão, sob a responsabilidade de cada usuário, devem ocorrer apenas em equipamentos e acessórios da Fusão. Qualquer exceção a esta regra deverá, obrigatoriamente, ser precedida da devida classificação da informação, da aprovação formal do Gestor proprietário da informação e do uso das proteções adequadas.

O usuário deve bloquear a tela da estação de trabalho sempre que se ausentar do seu Posto de Trabalho, utilizando funções de teclas (Ctrl+Alt+Del) previamente informadas pelo Departamento de TI.

Ao transportar os recursos móveis da Fusão (Laptops, iPads, Pendrives e telefone celular) nos meios de transportes público e pessoal (carro, avião, ônibus) o usuário deve adotar as medidas de cautela e proteção, de maneira a evitar sua exposição e a consequente cobiça de terceiros.

Os usuários devem zelar pelo perfeito funcionamento dos programas de proteção da estação de trabalho (antivírus, firewall, etc) e por isto, comprometer-se em não alterar as configurações desses programas, mesmo que tenha perfil para tal, de maneira a não colocar em riscos as informações e os ambientes da Fusão. Igualmente, caso perceba qualquer tipo de anormalidade, compromete-se em comunicar via e-mail o Departamento de TI o ocorrido.

A Fusão reserva-se o direito de efetuar verificações periódicas nas estações de trabalho para avaliar o nível de atualização do programa Antivírus da estação de trabalho. O usuário deve comunicar via e-mail o Departamento de TI qualquer anormalidade encontrada.

7. Utilização de Compartilhamentos e Grupos de Trabalho:

A permissão de acesso aos diretórios de rede segue políticas determinadas pelos gestores dos departamentos e não pelo Departamento de TI.

Toda solicitação de criação e compartilhamento de pastas/diretórios nos servidores, deve ser solicitada ao Departamento de TI pela gestor imediato e previamente aprovada pelo gestor. Estes diretórios (pastas) devem conter exclusivamente documentos e arquivos necessários ao desenvolvimento do trabalho.

O diretório (pasta) Público ou Temp não tem backup e toda semana, preferencialmente aos sábados, o conteúdo do diretório (pasta) público será apagado por processo automatizado pelo Departamento de TI.

O diretório Público ou Temp da rede é para transferência de arquivos não confidenciais e de forma temporária e devem ser utilizados para a troca de arquivos ao invés de usar o e-mail.

8. Engenharia Social:

É expressamente proibido qualquer tipo de discussão ou conversas (diretamente, por e-mail, por telefone, pelas redes sociais, entre outros meios) sobre assuntos confidenciais da Fusão, em locais externos e/ou na presença de pessoas não autorizadas, assim, deve ser assegurada de que não haverá outra pessoa não autorizada participando ou escutando a conversa.

9. Conclusões:

Cada funcionário tem o dever de contribuir, a seu nível, com a segurança geral. Para tanto, deve aplicar as disposições indicadas na presente Política de Segurança da Informação da Fusão. Qualquer anormalidade ou incidente (tentativa de violação do posto de trabalho ou de arquivos, roubo de equipamento, etc.) deve ser sinalizada imediatamente ao Departamento de TI.

A Fusão utiliza ferramentas de filtragem, controle e manutenção integrada aos sistemas de informação a fim de garantir a segurança da rede e de preservar os seus interesses legítimos.

A Fusão tem o direito de supervisionar a utilização dos recursos e controlar os acessos dos usuários no exercício de suas missões. Auditorias de controle serão realizadas para verificar a correta aplicação desta Política de Segurança da Informação.

O desrespeito às regras ou medidas constantes nesta Política de Segurança da Informação deverá ser investigado pelo Comitê de Ética e, desde que constatadas faltas imputáveis a algum(ns) usuário(s), responsabilizará individualmente o usuário e o submeterá a sanções disciplinares nos termos do Regimento Interno do Comitê de Ética.

O não cumprimento das regras previstas nesta Política de Segurança da Informação será encaminhado ao Comitê de Ética da Fusão e, se comprovada violação, o responsável será submetido as penalidades previstas no Regimento Interno do Comitê de Ética.

Recibo de Entrega DA POLÍTICA DE Segurança da Informação DA FUSÃO

Declaro para todos os fins de direito, ter recebido uma via da Política de Segurança da Informação da Fusão, que por ser um documento vivo, poderá sofrer atualizações, que me serão informadas pela Empresa, por meio de notas de difusão e/ou outros meios de comunicação internos da mesma, visando manter seguro o sistema de informação da Fusão. Declaro ainda, estar ciente de que o documento em referência se encontra disponível na Rede da Empresa para a minha consulta irrestrita e em qualquer tempo.

A Política de Segurança da Informação da Fusão foi lida por mim em sua íntegra e com a qual manifesto o meu aceite, comprometendo-me iteiramente com sua observância e, caso haja violação das disposições, concordo com a aplicação das penalidades previstas, em:

No artigo 482 da Consolidação das Leis Trabalhistas, que trata da ruptura do contrato de trabalho por justa causa;
Nos Termos de Compromisso de Estágio;
Nas regras contratuais de Prestação de Serviços;
No regimento interno do Comitê de Ética.