POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Última atualização: 27/11/2015

EXCLUSIVO PARA USO INTERNO

Produzido pelas áreas de Gestão, Compliance e TI-Infra.
Aprovado e revisado pelo Comitê de Compliance.

ÍNDICE

I. OBJETIVO

A Política de Segurança da Informação (”Política”) visa preservar a confidencialidade, integridade e disponibilidade das informações utilizadas pelas empresas da KSM (KSM) no desempenho de suas atividades, descrevendo a conduta adequada para o seu manuseio, controle, proteção e descarte, bem como estabelecer regras para acesso físico às instalações da KSM.

II. ABRANGÊNCIA

Esta política abrange todos os Colaboradores e Visitantes que possuam acesso à rede KSM, à informações confidenciais, aos equipamentos computacionais ou ambientes controlados que necessitem de um *login* ou cartão de acesso, para que lhe sejam disponibilizados tais informações.

Terão acesso às Informações Confidenciais e ambientes controlados da KSM, dentro dos limites definidos, os Colaboradores que concordarem com a política registrando o aceite através da assinatura do TERMO DE COMPROMISSO apresentado quando de sua admissão na KSM. Este termo determina a adesão do profissional a todas as políticas e normas internas, incluindo esta política.

III. CONCEITOS

Para efeitos da presente política, considera-se:

Rede KSM: Abrange todos os sistemas, diretórios e Intranet disponibilizados aos Colaboradores da KSM, conforme perfil de acesso definido.

Software: São todos os programas instalados nos computadores, os quais são disponibilizados pela equipe de TI INFRA para o exercício de sua função.

Homologação: Verificação pela equipe de TI INFRA quanto à compatibilidade técnica do software e aplicativos em relação ao parque tecnológico. Confirmação pelo usuário final do sistema do adequado funcionamento das funcionalidades previstas no quando da implantação ou da atualização de versão do mesmo.

Ambiente Lógico: ambiente controlado, eletrônico, onde circulam e são armazenadas Informações Confidenciais, softwares e sistemas.

Ambiente físico: dependências físicas das sociedades que integram a KSM.

Usuário: Colaborador ou Colaboradores que detenham acesso aos ambientes físico e lógico das sociedades da KSM para o desempenho de suas atividades.

Informações Confidenciais: São consideradas informações confidenciais, para os fins desta Política, quaisquer informações consideradas não disponíveis ao público ou reservadas, dados, especificações técnicas, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, software e documentação de computador,

comunicações por escrito, verbalmente ou de outra forma reveladas pela KSM em decorrência do desempenho de suas atividades.

Colaborador ou Colaboradores: todos os associados, prestadores de serviço e quaisquer prepostos das sociedades que compõem a KSM.

Associados: todos os profissionais que mantenham vínculo empregatício ou participação social em quaisquer das sociedades da KSM.

Prestadores de serviços: pessoa jurídica ou física que mantenha contrato de prestação de serviço, ou tenha celebrado instrumento afim com quaisquer das sociedades da KSM.

Visitante: todo indivíduo que não mantenha qualquer sorte de vínculo formal com as sociedades da KSM, enfim, todos aqueles que não se enquadram na definição de Colaborador, conforme acima.

IV. RESPONSABILIDADES

KSM

- Inclusão no planejamento orçamentário anual o valor de investimento em recursos computacionais, incluindo aquisição e renovação de equipamentos e softwares;
- Fornecer capacidade suficiente para realização dos Backups referentes aos processos e atividades da empresa;
- Fornecer espaço suficiente no SERVIDOR DE ARQUIVOS para armazenamento seguro de arquivos que contenham informações referentes aos processos e atividades da empresa;
- Indicação de suas necessidades de recursos de TI;
- Utilização dos recursos de TI de acordo com o Código de Ética da KSM;
- Utilização da ferramenta de Correio Eletrônico para uso profissional;
- Orientação às suas equipes quanto a aplicação das normas previstas nesta política.

EQUIPE DE TI - MODAL

- Administrar e atualizar a capacidade do Backup;
- Administrar e atualizar a capacidade de armazenamento;
- Auxiliar os departamentos com fornecimento de informação técnica dos recursos em uso;
- Realizar de segunda a sexta-feira o backup das caixas postais armazenadas no servidor Exchange;
- Execução das rotinas de backup e restauração de dados dos servidores.

V. POLÍTICA DE CONFIDENCIALIDADE

Neste item são definidas como serão tratadas as informações institucionais, forma de uso, possibilidade ou não de disponibilização ao ambiente externo ou a terceiros. Assim, sempre que

houver a necessidade de utilização de informações de conteúdo institucional, é necessário atentar-se para as determinações abaixo descritas:

V.1 PROPRIEDADE DAS INFORMAÇÕES E SOFTWARE

Os softwares adquiridos no mercado ou desenvolvidos internamente pertencem exclusivamente à KSM, bem como todos os direitos relativos a todas as invenções, inovações tecnológicas, elaboradas e/ou desenvolvidas pelos Colaboradores, durante a vigência da relação de emprego ou contrato, ou quando forem utilizados recursos, dados, meios, materiais, instalações, equipamentos, informações tecnológicas e segredos comerciais, pertencentes à KSM, sendo vedada a cópia ou disponibilização através de qualquer meio (eletrônico ou físico) para ambiente externo à KSM.

Toda estrutura mantida pela KSM, composta pela rede, telefonia, correio eletrônico, internet e outros meios de comunicação, são instrumentos de trabalho de sua propriedade que o mesmo disponibiliza aos Associados e Colaboradores a fim de tornar suas tarefas mais eficientes. Da mesma forma, todos os documentos, estejam eles em forma impressa ou eletrônica, ou que circulem por estes meios, também são de propriedade da KSM e todos devem envidar esforços para protegê-los de uso indevido. É proibido o uso destes documentos fora da KSM cujo objetivo não seja atender, exclusivamente, aos interesses da instituição, e, ainda assim, sua retirada ou envio somente poderá ser efetuado com autorização de um dos sócios. Sua retirada ou envio com qualquer outra finalidade constitui violação a esta política. A sua transmissão via correio eletrônico, fax ou outro meio, deverá ser feita com o máximo de atenção e seguindo as regras de segurança e confidencialidade constantes nesta Política e no Código de Ética. Os documentos alterados fora da KSM devem ter seus arquivos, manuais ou na rede, atualizados imediatamente.

V.2 CLASSIFICAÇÃO DA INFORMAÇÃO

As informações que transitam pela KSM são, para fins desta Política, classificadas em quatro padrões distintos, a saber:

INFORMAÇÕES PÚBLICAS: Aquelas destinadas a disseminação fora da KSM. Possuem caráter informativo geral e são direcionadas a clientes ou investidores. Exemplos: material de marketing, *clipping information*, registros regulamentares e da Comissão de Valores Mobiliários.

INFORMAÇÕES INTERNAS: São aquelas destinadas ao uso dentro da KSM. A divulgação de informações desta natureza, ainda que não autorizada, não afetaria significativamente a KSM ou seus clientes e associados. Essas informações não exigem proteções especiais salvo aquelas entendidas como mínimas para impedir a divulgação externa não intencional.

INFORMAÇÕES CONFIDENCIAIS: Também destinam-se a uso interno da KSM. Entretanto, diferem das informações de natureza interna à medida que sua extensão em uma eventual divulgação, poderia afetar significativamente os negócios da KSM, seus clientes, investidores e associados. Exemplos: registros de funcionários, planos salariais, informações sobre clientes, sejam elas genéricas ou específicas, classificação de crédito, saldos de contas-correntes. Sua divulgação é proibida, salvo se solicitada por órgão fiscalizador competente (BACEN, CVM e Receita Federal, por exemplo), situação na qual deverá ser prestada por uma das seguintes pessoas: Contador, Controller, Auditor Interno, Advogado ou um dos sócios.

INFORMAÇÕES ALTAMENTE RESTRITAS: Correspondem a mais alta classificação de segurança para as informações que transitam na KSM. Destina-se às informações cuja divulgação não autorizada, provavelmente provocaria danos substanciais, constrangimentos ou penalidades aa KSM, seus clientes, investidores ou associados. As pessoas designadas para o trato e uso de tais informações, têm a responsabilidade de garantir que elas sejam devidamente protegidas e seguramente armazenadas quando não estiverem em uso. Exemplos: informação antecipada e não autorizada de novos produtos ou serviços, informações de fusões, aquisições ou outras atividades do mercado de capitais não disponíveis ao público em geral.

Em função desta categorização, é possível, quando do envio de informações sensíveis, a utilização de funcionalidade do Outlook, que permite classificar arquivos e mensagens conforme sua criticidade, que devem ser considerados sempre quando o mesmo for disponibilizado ou encaminhado para terceiros.

Sempre que forem trocadas informações sensíveis, orienta-se a utilização de senhas, sistemas de criptografia ou EDI (*Eletronic Data Interchange*) minimizando riscos de que informações sensíveis da KSM sejam acessadas por terceiros.

VI. POLÍTICA DE PRIVACIDADE

VI.1 CORRESPONDÊNCIA ELETRÔNICA

Tal como telefone, fax, carta e outros documentos, o e-mail também é forma de comunicação de uso da KSM, cujo objetivo é tornar suas atividades mais rápidas e fáceis. O e-mail também caracteriza um compromisso com terceiros, sejam eles clientes ou prestadores de serviço, e equivale aos papéis timbrados da KSM, portanto, o uso desta ferramenta deve ser feito de forma cautelosa, profissional e com linguagem adequada.

A KSM utiliza um padrão de *auto-signature* em cada correspondência eletrônica enviada, visando a mesma proteção legal das mensagens enviadas por fax. É expressamente proibida a alteração ou exclusão deste padrão de *auto-signature*.

Como se trata de ferramenta de trabalho de propriedade da KSM, todos os e-mails enviados, principalmente aqueles com arquivos anexados, devem ser rigorosamente checados e enviados com o máximo cuidado com relação ao destinatário para evitar que informações confidenciais ou de uso restrito se extraviem.

Com relação ao uso do e-mail, algumas práticas são proibidas. São elas:

i) Assediar ou perturbar outrem seja através de linguagem inadequada, alta frequência de mensagens ou excessivo tamanho de arquivos;
ii) Enviar quantidade excessiva de mensagens de e-mail em lote ("*junk mail*" ou "*spam*") ou e-mails mal-intencionados ("*mail bombing*") que, de acordo com a capacidade técnica da rede, seja prejudicial ou sobrecarregue intencionalmente usuários, site, servidor, etc;
iii) Reenviar ou, de qualquer forma, propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens; e
iv) Cadastrar em sites de compras e entretenimentos o e-mail corporativo como contato.

A KSM adota o *software* SOPHOS, através do qual realiza o filtro para verificação de mensagens recebidas e enviadas por seus Associados, com o intuito de minimizar os riscos de ataques externos (cavalos de Tróia e vírus), que conteúdos não autorizados ou ilegais possam chegar a sua rede ou que Informações Confidenciais sejam indevidamente encaminhadas a terceiros.

VII. POLÍTICA DE SENHAS E DIREITO DE ACESSO

VII.1 SENHAS

A senha é a chave de acesso pessoal que garante que somente pessoas autorizadas utilizem determinados dispositivos ou recursos. Cada usuário é responsável pela manutenção e guarda de sua senha, a qual não pode ser compartilhada e não deve ser anotada em arquivos físicos ou de fácil acesso. Cabe aos usuários a memorização de suas senhas, sendo sugerida a não utilização de códigos comuns, tais como: o próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário e números sequenciais, etc.

Mecanismos para elaboração de senhas:

- Utilize preferencialmente senhas distintas para usos distintos, evitando repetir senhas de uso pessoal para acessos corporativos.
- Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Desta forma, evite o uso de dados pessoais, sequencias de teclado, palavras que fazem parte de listas publicamente conhecidas (times de futebol), por exemplo.
- Selecione caracteres de uma frase: “Eu trabalho no Banca KSM há 3 anos e 1 mês”: EtBMh3a.1m
- Utilize uma frase longa, como parte de uma música, por exemplo: “Ninguém segura a juventude do Brasil”
- Faça substituição de caracteres semelhantes: “Astro-rei” por “A5tr0-re1”

VII.2. ACESSO A DIRETÓRIOS

Todos os associados quando admitidos receberão um perfil básico, o qual dará acesso aos seguintes diretórios:
DPTO: onde ficam armazenados os arquivos relativos aos projetos
DPTO/Socios: ficam armazenados os arquivos de interesse exclusivo da sociedade
IMPRESSORAS: onde ficam armazenados os arquivos digitalizados nas impressoras locais
PUBLICO: diretório temporário para uso comum dos diversos usuários
ADM: diretório de administração do TI Modal para o gerenciamento do rede, backups e restores

VII.3. ACESSOA À REDE VIA WI-FI (WIRELESS FIDELITY)

O acesso à rede interna via Wi-Fi só é permitida para os Sócios e para visitantes externos que utilizarão as salas de reunião para apresentações ou auditorias.

Este acesso é vedado para os demais associados.

VII.4 INTERNET

O acesso à Internet é permitido a todos os Associados usuários de computador, com o objetivo de facilitar suas tarefas. Assim como qualquer outro material de trabalho, as páginas da Internet também devem ser usadas somente para fins profissionais.

Para uma utilização eficiente e produtiva algumas regras devem ser obedecidas:

- É proibido o acesso a sites ilegais ou não autorizados, tais como os relacionados a sexo, pornografia, pirataria, atividades de hacker e quaisquer outras atividades ilegais. Estes exemplos não esgotam a lista de sites proibidos, portanto quaisquer dúvidas devem ser levadas ao conhecimento da área de TI - HelpDesk.
- Fica proibido também o download de arquivos e programas não autorizados ou sem revisão e aprovação da TI - Infra.

A intenção desta política é evitar que vírus, cavalos de Tróia e outros programas indevidos, não licenciados e nocivos apareçam no ambiente de computação da KSM.

VII.5 PROCEDIMENTOS DE RETIRADA DE ACESSO

Quando um Associado é desligado da KSM, ele perde imediatamente o direito de acesso aos diversos ambientes de rede, serviço de e-mail externo e internet.

Os trabalhos desenvolvidos ou elaborados pelo Associado pertencem exclusivamente a KSM, não cabendo ao associado o direito de retirá-lo ou copiá-lo quando de seu desligamento, não sendo permitida a gravação de arquivos em qualquer mídia sem a devida autorização por parte dos sócios.

VIII. POLÍTICA DE BACKUP

O backup do servidor de arquivos, exchange e Active Direct é realizado diariamente e mensalmente através de processo automatizado, em fita, sendo encaminhados para armazenamento junto a prestador de serviço de guarda especializado, devidamente contratado pelo MODAL para este fim, no dia seguinte (D+1).

O Backup do Exchange/emails também é realizado diariamente. A retenção de emails deletados é de 07 (sete) dias.

IX. POLÍTICA DE USO ACEITÁVEL

IX.1 SOFTWARE E COMPUTADORES

Para mantermos o ambiente lógico, todos os softwares/aplicações operacionais devem ser homologados pelos usuários das áreas envolvidas, que devem verificar os impactos das novas versões nos procedimentos, resultados e obrigações.

Aquisição: A aquisição de softwares ocorrerá conforme planejamento orçamentário, com base na homologação técnica por parte da equipe de TI, após validação das necessidades de uso pela diretoria da empresa.

Instalação: Somente a equipe de TI INFRA está autorizada a realizar instalação de qualquer tipo de software, seja este um sistema ou um aplicativo simples, principalmente aqueles obtidos gratuitamente e/ou baixados da internet.

Licença de Uso: Somente poderão ser instalados e utilizados softwares devidamente licenciados para uso da KSM. Não é permitido instalar softwares pessoais, emprestados, de terceiros, que não sejam devidamente licenciados para uso da KSM pelo fabricante do produto.

Auditoria: Poderá ser utilizada pela equipe de TI INFRA uma ferramenta automatizada para auditoria de softwares instalados nos computadores.

Marcas e Modelos: Utilização de equipamentos padronizados pela equipe de TI INFRA.

Propriedade: Os softwares, incluindo os desenvolvidos internamente, e recursos computacionais diversos pertencem exclusivamente a KSM, bem como todos os direitos relativos a todas as invenções, inovações tecnológicas e criações intelectuais elaboradas e desenvolvidas pelos Colaboradores, Prestadores de Serviços e Consultores, durante a vigência da relação de emprego ou relação contratual.

IX.2 SISTEMAS INTERNOS E APLICATIVOS

A KSM somente utiliza softwares aprovados e licenciados na execução de suas tarefas, não sendo permitido o uso pelos Associados de softwares que contrariem esta norma.

O uso de software não licenciado é crime previsto na Lei 9.609 de 19 de fevereiro de 1998. Além disso, existe um risco considerável na utilização de quaisquer softwares externos ao ambiente, destes possuírem vírus ou outras ameaças de segurança escondidas.

A instalação de softwares autorizados e cópias de arquivos para uso fora da KSM, *em pen drives*, cds, USB ou em outras mídias, deve ser autorizadas pelo Sócio Responsável pela área, bem como pelo Compliance. É proibida a execução destas tarefas por Associado que não pertença à área de TI Infraestrutura.

IX.3 VÍRUS

A qualquer indício de existência de vírus, o Associado deve interromper suas tarefas e comunicá-lo imediatamente à TI Infraestrutura, que executará os procedimentos para a erradicação de vírus determinados na Política de Segurança.
Os esforços individuais e isolados dos usuários para acabar com os vírus podem contribuir para provocar danos ainda maiores, pois, em geral, estes usuários não estão capacitados para esta atividade.

O uso de softwares freeware ou shareware e arquivos em outras mídias constituem formas muito comuns de transferência de vírus para os computadores, portanto, sua utilização sem a prévia autorização da TI Infraestrutura é terminantemente proibida.

Além dos programas que protegem a rede, todos os computadores possuem software de verificação de integridade (agente do antivírus), que detecta alterações nos arquivos de configuração e nos softwares e alertam ao usuário da possibilidade de existência de vírus. Isso ocorrendo, o mesmo deve notificar a TI - Infra imediatamente.

Todos os equipamentos utilizados para gravação de informações em computadores ligados à Rede KSM deverão ser apresentados ao Departamento de TI para verificação e certificação da inexistência de vírus que possam ocasionar danos estrutura da Rede KSM.

X. NOTIFICAÇÃO DE INCIDENTES E ABUSOS

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas e redes. Alguns exemplos são: tentativa de uso ou acesso não autorizado a sistemas e dados, tentativa de tornar serviços indisponíveis, desrespeito à política de segurança.

É responsabilidade dos Associados notificar a área de Risco Operacional ou Compliance, sempre que se deparar com uma atitude que considere abusiva ou com um incidente de segurança para que sejam tomadas as devidas ações, minimizando os impactos da ocorrência.