POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DATA: 25/01/2016

VERSÃO 2.0

SUMÁRIO

I. INTRODUÇÃO

Nesta política de Segurança da Informação constam as práticas e cuidados mínimos necessários aplicáveis a todos os colaboradores da Meta Asset Management ("Meta") no manuseio, guarda, descarte e transmissão dos ativos de informação, dos clientes ou da empresa, respeitando as definições e conceitos estabelecidos.

Um sistema de informações, transparente e eficaz, se constitui num ativo muito importante, sobretudo em empresas pertencentes ao mercado financeiro e de capitais.

A Meta depende de seus ativos de informação para realizar negócios e atender suas obrigações operacionais, comerciais e estratégicas. Estes sistemas de informação, bases de dados, equipamentos, tecnologia e documentos em geral, sejam eles internos ou externos, devem ser protegidos.

Para efeito desta política, são considerados como "ativos de informação", todas as informações em quaisquer meios utilizados pela Meta, bem como todos os equipamentos e instalações onde são manuseadas, acessadas ou armazenadas.

Estamos comprometidos e cientes de que a implementação de uma estrutura de controles formal, para gerir a segurança de nossas informações (e dos nossos clientes), é um passo essencial para estabelecer os níveis de controle e responsabilidade necessários para preservar os ativos de informação e constituir um diferencial aos nossos negócios.

Seguindo os conceitos das boas práticas de controles e de segurança da informação, esta política interna da Meta foi elaborada com intuito de prezar pela segurança, bom uso e acesso controlado a determinadas informações, recursos e pessoas.

A seguir estão transcritas algumas importantes regras e diretrizes que são atentamente observadas por todos os sócios, profissionais e funcionários ("colaboradores") da Meta Asset Management.

II. PAPÉIS E RESPONSABILIDADES

II.1 - COMITÊ EXECUTIVO

Disseminar a importância e estar engajado quanto ao cumprimento do conteúdo desta Política, bem como gerenciar a observância de conformidade através da revisão contínua de relatórios periódicos, participação em reuniões internas, treinamentos, dentre outras atividades.

II.2 - CONTROLES INTERNOS

As principais atribuições deste segmento da Meta, no tocante à segurança das informações, são:

- **Gerenciar as ações em segurança das informações físicas e lógicas;**

Conscientizar os funcionários através de treinamentos, apresentações de casos e demonstração de boas práticas;

Monitorar as atividades de administração de acesso físico e lógico;

Mapear processos e descrever procedimentos e rotinas operacionais;

Analisar potenciais ameaças e estabelecer mecanismos de controles que minimizem eventuais vulnerabilidades de segurança detectadas; e

Elaborar e atualizar regras e procedimentos referentes à segurança da informação.

II.3 – ADMINISTRATIVO (SERVIÇOS GERAIS, EXPEDIÇÃO E RECEPÇÃO)

Contratar e atualizar apólice de seguro de bens e recursos da Meta;

Administrar a segurança física e a prestação de serviços de manutenção e limpeza terceirizados (quando aplicável);

Identificar bens e recursos como patrimônio da empresa;

Gerenciar os serviços de expedição de documentos e correspondências;

Monitorar continuamente e assegurar que os ambientes onde há compartilhamento de informações tenham acesso restrito;

Gerenciar os procedimentos inerentes à identificação de funcionários, terceiros e visitantes da Meta;

Assegurar a segurança e bom uso dos locais destinados para armazenamento de documentos, mídias, dentre outros.

II.4 – RECURSOS HUMANOS

Comunicar e atualizar, tempestivamente, todas as informações referentes à movimentação de pessoal;

Organizar treinamentos em segurança da informação e de melhores práticas quanto ao uso de recursos de tecnologia;

Aplicar as penalidades previstas no Código de Conduta e Ética da Meta; e

Providenciar a adesão a termos de confidencialidade e normas internas da Meta de todos os novos funcionários e/ou demais profissionais terceirizados, quando for o caso.

II.5 – TECNOLOGIA DA INFORMAÇÃO

Em relação à segurança da informação, as principais funções são:

Desenvolver programas regulares de avaliação de riscos de tecnologia com acompanhamento da área de Controles Internos;

Seguir procedimentos rígidos que garantam a base tecnológica para recuperação de desastres e continuidade dos negócios da Meta;

Homologar novos recursos de tecnologia, para a segurança das informações, conforme definido pela empresa;

Realizar gravação telefônica dos ramais necessários e o backup diário de informações, mantendo em arquivo seguro e organizado durante os prazos legais e/ou internos;

Criar processos que garantam a verificação dos registros de atividades ("logs") em todos os sistemas e recursos de tecnologia e dados; e

Informar, registrar e tratar incidentes de tecnologia relacionados à segurança das informações ou continuidade dos negócios.

II.6 – JURÍDICO

Revisar contratos garantindo a existência de cláusulas referentes à confidencialidade e segurança das informações; e

Elaborar termos de confidencialidade e responsabilidade.

II.7 - COMERCIAL

Assegurar a confidencialidade das informações e documentos pessoais de clientes sob sua responsabilidade.

III. GESTÃO DE ACESSOS FÍSICOS E LÓGICOS

III.1 - ACESSO LÓGICO

O acesso aos sistemas internos e externos deve ser solicitado ao gestor da área do colaborador solicitante;

Após aprovação, cabe ao responsável por Segurança das Informações avaliar a solicitação e conceder o acesso solicitado;

Semestralmente, o responsável por Segurança das Informações deve revisar os usuários cadastrados para deliberar sobre a manutenção, revisão ou revogação dos perfis de acesso existentes;

Na eventualidade de transferências ou alterações de cargo, função ou área, os perfis de acesso são revisados;

Ao responsável pela gestão dos Recursos Humanos, cabe a responsabilidade de informar tempestivamente, para

providências da área de TI, períodos de ausências programadas de colaboradores (férias, licenças em geral, dentre outras);

As providências de TI mencionadas em epígrafe, dentre outras, são as de bloquear acesso a sistemas, rede corporativa e serviço de e-mail durante o período de ausência do colaborador; e

Na hipótese de desligamento de algum colaborador, todos os acessos são imediatamente bloqueados.

III.1.1 – POLÍTICA DE SENHAS

A senha é de uso pessoal e intransferível;

O eventual uso ou acesso indevido é de total responsabilidade do detentor e titular da senha que deve tomar todos os cuidados necessários para salvaguardá-la;

O compartilhamento de senhas somente será permitido em casos de indisponibilidade para uso individual e se aprovado prévia e formalmente;

Toda e qualquer senha, de acesso físico ou lógico, deverá ser imediatamente bloqueada em casos de desligamento, suspensão, demissão, férias ou licenças de funcionários;

Quanto às características e complexidade, a senha:

Deve possuir, no mínimo, 8 (oito) caracteres e entre letras, números e caracteres especiais;

Deverá ser alterada, compulsoriamente, a cada 60 (sessenta) dias; Deverá mesclar entre letras maiúsculas e minúsculas;

Não pode ser igual ou similar às 3 (três) últimas utilizadas; Não pode conter nome completo, apelido ou o login;

Após 3 (três) tentativas, em caso de insucesso, ser automaticamente bloqueada;e

Sendo nova, o usuário deverá, obrigatoriamente, alterá-la no primeiro acesso seguindo os critérios acima citados.

III.2 - ACESSO FÍSICO

É proibida a entrada de ex-colaboradores sem expressa autorização de um sócio responsável;

Quaisquer terceirizados ou fornecedores somente poderão prestar os serviços solicitados com o devido acompanhamento de algum colaborador da Meta;

Outras pessoas, além das acima mencionadas, somente podem ter acesso às dependências da Meta com a ciência do responsável da área ou a quem este previamente autorizar;

Colaboradores ou visitantes que necessitarem sair das dependências físicas portando quaisquer documentos, recursos ou materiais de propriedade da Meta devem ser expressamente autorizados; e

Os arquivos físicos, principalmente os que contemplam documentos e informações de clientes da Meta, são de acesso controlado e restrito somente aos colaboradores autorizados.

IV. ARMAZENAMENTO E TRATAMENTO DE DADOS E INFORMAÇÕES

Cada funcionário da Meta é responsável direto pela guarda e verificação da integridade dos arquivos, documentos, planilhas, relatórios, dentre outros;

O arquivamento externo, quando houver, seja de mídias ou documentos físicos, deve ser objeto de formalização contratual e ser periodicamente submetido à avaliação e visita presencial;

Locais destinados ao armazenamento de informações de clientes, confidenciais ou relevantes, devem permanecer em locais (físicos ou lógicos) de acesso restrito, seguros e organizados quando não estiverem sendo manuseados;

Não é recomendado o uso do e-mail para o armazenamento de informações relevantes. Estas deverão ser arquivadas na rede corporativa para assegurar o efetivo procedimento de backup dos dados em caso de contingência ou incidente;

Os arquivos lógicos ou físicos com informações de clientes, relevantes ou confidenciais devem ser descartados através do uso de máquinas fragmentadoras específicas para este fim;

O envio de informações e documentos em meio físico para locais externos deve ser necessariamente protocolado (entrada e saída) e arquivado para fins comprobatórios e de rastreamento, quando necessário; e

Relatórios de auditorias, órgãos reguladores ou fiscalizadores são de propriedade da Meta e, consequentemente, estritamente confidenciais.

IV.1 – BACKUP DE DADOS E INFORMAÇÕES DA META

A prática e as rotinas diárias de backup visam assegurar a disponibilidade das informações geradas ou utilizadas pela Meta, inclusive e prioritariamente, a de seus clientes.

O período de armazenamento de informações, antes do descarte definitivo, deve respeitar os períodos exigidos por leis, normas e regulamentos aplicáveis aos negócios da Meta.

Para assegurar a segurança, organização e periodicidade de guarda dos dados, a Meta possui procedimentos de backup que compreendem: cópia, armazenamento e recuperação de suas informações e, principalmente, de seus clientes.

É vedada, aos usuários, a prática de armazenamento de dados e informações em disco local, cabendo aos mesmos a responsabilidade de manipular e salvar arquivos lógicos somente na rede corporativa da Meta.

IV.2 - USO DE RECURSOS DE TECNOLOGIA

A Meta é proprietária do direito de uso de todos os recursos de tecnologia colocados à disposição dos colaboradores, bem como de toda a informação criada e gerada durantes as atividades profissionais ou nas dependências da empresa.

Os recursos de tecnologia da Meta abrangem: computadores, notebooks, impressoras, scanner, aparelhos de softwares, periféricos, telefonia e mídias em geral.

É expressamente proibida, portanto, a utilização de quaisquer recursos de tecnologia que não sejam de propriedade da Meta, tais como: recursos de multimídia, monitores, notebooks, HD externo, pen drives e demais mídias removíveis, impressoras, etc.

Os usuários de recursos portáteis deverão atestar, através de assinatura de um termo de responsabilidade específico, que tomarão todos os cuidados necessários no transporte e utilização destes equipamentos. Ainda, se comprometem a cumprir a função obrigatória de armazenar, na rede corporativa, todas as informações disponíveis nestes recursos.

O bom e correto uso dos recursos de tecnologia é responsabilidade de todos os funcionários da Meta.

IV.3 - UTILIZAÇÃO DO E-MAIL E TELEFONIA

O funcionário deve prezar pela boa e responsável utilização de sua conta de e-mail corporativo;

Na Meta, o uso para fim pessoal é permitido, todavia, deve ser de caráter resumido e objetivo;

Não é permitida a utilização do e-mail para envio de e-mails em massa, correntes, convites, cartões virtuais, promoções pessoais e outros assuntos não relacionados às atividades profissionais e aos negócios da Meta;

Em nenhuma hipótese devem ser acessados e-mails de remetentes ou assuntos desconhecidos;

O correio eletrônico não pode ser utilizado, sem autorização prévia e controle específico, para envio ou recepção de mensagens que contenham arquivos executáveis, macros ou seqüências de comandos, explícitas ou implícitas, ou ainda outros mecanismos que possam conter vírus e, portanto, causar algum dano aos equipamentos da Meta ou de seus destinatários;

É expressamente proibido o uso do e-mail corporativo para participação em blogs, redes sociais (Ex. Twitter, Facebook), serviços de webmail ou mensageria, cadastramento em sites para fins pessoais (lojas virtuais, bankline, chats, dentre outros);

Cabe ainda ressaltar que é proibido o envio, recepção ou encaminhamento de mensagens com teor ofensivo, ideologias políticas, religiosas ou raciais, pornografia, apologia às drogas, terrorismo, dentre outros considerados impróprios;

Quanto às assinaturas de e-mail, somente é permitido o uso do padrão interno previamente definido (inclusive formato e ordem das informações); e

Atendimento a clientes e realização de operações, devem ser realizados somente através de ramais gravados.

IV.4 - INFORMAÇÕES PRIVILEGIADAS

As conseqüências do uso de informações privilegiadas p odem ser graves, tanto para o funcionário quanto para a Meta.

Informações privilegiadas podem incluir, mas não se limitam, a informações relacionadas com propostas ou contratos de fusão e aquisição, modificação na situação financeira, previsões ou projeções financeiras, oferta ou transações de títulos e valores mobiliários, licitações, informações sobre crédito, alterações de dividendos, desinvestimentos, processos de falência, litígios substanciais, alterações na administração, desenvolvimento de produtos, anúncios de lucros, novos comunicados ou outros eventos significativos a respeito de um emitente.

Importante esclarecer que informações privilegiadas também podem se referir a eventos futuros ou passados.

Algumas regras básicas quanto ao cuidado no tratamento de informações privilegiadas, são:

É vedado, ao funcionário, compra, venda ou recomendação de títulos e valores mobiliários de um emissor ou cotas de um fundo de investimento para qualquer conta própria, de cliente, de funcionário ou outra quando estiver de posse de informações relevantes e não disponíveis ao público ("informações privilegiadas"), devendo realizar todas as

atividades de investimentos de acordo com as leis, normas e regulamentos aplicáveis;

É expressamente proibida a compra, venda, recomendação ou comercialização, de qualquer título, valor mobiliário ou cotas de fundos de investimentos, tanto pessoalmente quanto em nome de outros, na eventualidade do funcionário possuir informações privilegiadas relacionadas a tal título/fundo;

Os funcionários estão orientados a indicar, como "informação confidencial", todas as informações privilegiadas relevantes e não disponíveis ao público; e

Todas as informações privilegiadas que forem obtidas ou acessadas durante ao exercício pleno e responsável das atividades deverão ser manuseadas, armazenadas e descartadas conforme o previsto nesta Política e nas leis e normas em vigor.

V. INCIDENTES

Diante de uma eventual suspeição de fraude ou incidente que comprometa a segurança das informações da Meta ou no caso de ocorrência de um "vazamento" de informações ou incidente de segurança, o funcionário deve registrar e comunicar o fato imediatamente à área de Controles Internos e à Diretoria.

VI. CÓDIGO DE ÉTICA E CONDUTA

O Código de Ética e Conduta da Meta estabelece as diretrizes gerais e profissionais de conduta esperadas de todos os funcionários em suas relações entre si, com clientes, prospects, concorrentes, fornecedores, prestadores de serviços e com toda a sociedade.

A plena observância das diretrizes constantes ao longo do Código é premissa fundamental também para minimização dos riscos inerentes à segurança de nossas informações.

VII. TREINAMENTO

Todos os funcionários deverão, além de aderir a esta Política, receber treinamentos e materiais educativos que visem, principalmente, a conscientização de todos sobre o tema.

Novos funcionários devem ser submetidos a um treinamento inicial acerca de suas funções e responsabilidades quanto ao assunto.

É responsabilidade, da área de Recursos Humanos, efetuar o registro e o controle formal sobre o comparecimento das pessoas aos treinamentos e palestras, indicando a freqüência e o tipo de treinamento ministrado.

O treinamento deve ser ministrado por profissional interno (ou terceirizado)
com experiência comprovada quanto à gestão de segurança da informação.

VIII. PENALIDADES

A não observância do disposto nesta política interna será considerada como falta grave de acordo com o Código de Conduta e Ética da Meta.