MRB | CAPITAL

MRB CAPITAL GESTORA DE RECURSOS LTDA.

POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

Dezembro de 2017

MRB | CAPITAL

OBJETIVO

1.1. O objetivo da presente Política de Segurança da Informação da MRB Capital Gestora de Recursos Ltda. ("Política" e "Sociedade", respectivamente) é definir as regras para o uso adequado das informações e dos recursos de tecnologia da informação da Sociedade.

2. ESCOPO DE ATUAÇÃO

2.1. A Sociedade utiliza ferramentas e tecnologias para garantir que sua infraestrutura de tecnologia esteja em linha com as melhores práticas em termos de segurança e confiabilidade. Os procedimentos de segurança dos sistemas aplicados pela Sociedade são revistos continuamente e atualizados sempre que necessário.

2.2. O departamento de tecnologia da Sociedade é responsável por realizar, periodicamente, testes de segurança e procedimentos para detectar falhas e vulnerabilidades. Ainda, periodicamente são realizados treinamentos com os funcionários sobre o uso apropriado da infraestrutura de tecnologia.

2.2. As principais práticas de segurança da informação adotadas pela Sociedade têm como objetivo inibir:

(i) a transmissão não autorizada de informações confidenciais sobre clientes, colaboradores ou sobre a Sociedade;

(ii) cópia ou transmissão não autorizada de softwares ou dados proprietários;

(iii) acesso não autorizado a arquivos, comunicações e outros dados confidenciais relacionados aos clientes, colaboradores ou à Sociedade;

(iv) tentativas de interceptação de e-mail ou mensagem instantânea da Sociedade;

(v) ataques cibernéticos à Sociedade; e

(vi) liberação não autorizada de senhas e códigos de ID de usuários.

2.3. A Sociedade concede aos seus colaboradores acesso a seus sistemas, dados e instalações conforme a necessidade e as atividades efetivamente desempenhadas. Não obstante, os colaboradores da Sociedade devem sempre proteger adequadamente suas estações de trabalho, senhas, acessos pessoais e informações confidenciais sob sua responsabilidade e devem utilizar adequada e profissionalmente a infraestrutura de tecnologia da Sociedade. Os colaboradores da Sociedade têm o dever de reportar imediatamente qualquer indício de falha, invasão ou comportamento suspeito dos sistemas da Sociedade.

2.4. Todas as informações estratégicas da Sociedade, enquanto não divulgadas de forma oficial, são consideradas estritamente confidenciais. Os colaboradores Sociedade são responsáveis por garantir a segurança da informação sob a sua guarda.

2.5. O departamento de tecnologia da Sociedade é responsável por tomar as medidas cabíveis para avaliar e mitigar os danos em caso de falhas identificadas. Conforme necessário, incidentes relevantes devem ser escalados para a Diretoria de Compliance para que sejam avaliadas as implicações legais e regulatórias, bem como as ações corretivas apropriadas.

3. ABRANGÊNCIA

3.1. Esta Política deve ser observado por todas as áreas da Sociedade e por todos os agentes envolvidos em seus negócios.

4. RESPONSABILIDADES

4.1. A presente Política encontra-se sob responsabilidade da Diretoria de Compliance, cujas competências incluem:

(i) atualização periódica da presente Política;

(ii) testes periódicos de um plano de contingência,

(iii) solução de dúvidas e questões não contempladas pela Política;

(iv) avaliação e deliberação sobre a viabilidade econômico-financeira de projetos apresentados pelo departamento de tecnologia da Sociedade; e

(v) aprovação de alterações nesta Política.

5. CRITÉRIOS E REGRAS

PROPRIEDADE E PROTEÇÃO DA INFORMAÇÃO

5.1. Toda a informação produzida na Sociedade, ou por ela adquirida, é considerada de sua propriedade, sendo parte do seu patrimônio, não importando a forma de apresentação ou armazenamento. Esta informação deve ser adequadamente protegida e utilizada apenas no interesse da Sociedade. Seu uso ou divulgação externa somente poderá ocorrer quando expressamente autorizado pelo Diretor de Compliance.

5.2. A Sociedade poderá monitorar o recebimento, envio e conteúdo de todos os e-mails, arquivos e documentos de sua propriedade sem prévia notificação aos seus Colaboradores (conforme definido abaixo).

DIVULGAÇÃO

5.3. A Sociedade disponibilizará esta Política no portal de documentos internos da Sociedade para acesso de todos os seus sócios, funcionários e diretores ("Colaboradores") e disponibilizará uma cópia desta Política no ato da admissão de cada um de seus novos Colaboradores.

CONTRATOS DE SERVIÇOS (TERCEIROS)

5.4. Deve ser prevista nos contratos de prestação de serviços, cláusula específica expondo a obrigatoriedade do cumprimento da Política pelo fornecedor contratado pela Sociedade, para o qual deverá ser disponibilizada uma cópia de sua Política.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

6.1. Informações estratégicas da Sociedade, enquanto não divulgadas de forma oficial, são consideradas estritamente confidenciais.

6.2. O Colaborador é responsável por garantir a segurança da informação sob a sua guarda.

6.3. Não é permitido divulgar informações confidenciais, seja através de conversas informais, e-mails ou qualquer outro meio de comunicação, sem a prévia autorização.

7. SEGURANÇA FÍSICA E DO AMBIENTE

ACESSO FÍSICO

7.1. O acesso físico ao ambiente de tecnologia da informação somente será permitido por pessoas autorizadas pelo Diretor de Compliance.

7.2. O acesso às dependências da Sociedade em horários alternativos deverá ser previamente informado ao Diretor de Compliance, que tomará as providências necessárias.

ZELO COM AS INFORMAÇÕES

7.3. A informações classificadas como confidenciais e/ou estratégicas não devem ser deixadas sobre a mesa de trabalho, devendo ser armazenados dentro de gavetas ou armários.

7.4. As informações confidenciais devem ser totalmente destruídas quando não mais necessárias, independentemente do tipo de mídia em que estiverem armazenadas.

7.5. As impressões no ambiente de trabalho serão controladas por senha individual. Os arquivos que permanecerem na fila de impressões serão excluídos ao final do expediente.

7.6. O Colaborador deve sempre bloquear sua estação de trabalho quando interromper o uso, mesmo que por breves momentos.

7.7. O armazenamento de arquivos é bloqueado no disco local dos computadores, devendo ser utilizados os *drives* da rede para tal, onde dispositivos de segurança asseguram o correto tratamento desta informação.

7.8. Computação Móvel/Computação de Terceiros:

(i) O acesso a computação móvel será permitido somente para Diretoria;

(ii) Os prestadores de serviços terceirizados alocados na Sociedade deverão utilizar equipamentos fornecidos pela própria Sociedade; e

(iii) Caso os prestadores de serviços utilizem equipamentos próprios, estes somente terão acesso à rede *wireless guest*, desde que seu equipamento atenda aos requisitos mínimos de segurança previstos nesta Política.

7.9. Exceções ao disposto acima deverão ser aprovadas pela Diretoria de Compliance.

8. OPERAÇÃO DO AMBIENTE COMPUTACIONAL:

8.1. Operação dos Recursos de Processamento das Informações:

(i) **Conexões de Rede**

- Equipamentos conectados à rede *wireless* devem ter antivírus atualizadas;
- A Sociedade poderá auditar os equipamentos dos Colaboradores e prestadores de serviços para garantir a segurança geral de seu ambiente computacional sem prévio aviso;
- E proibido utilizar conexão discada via modem, ADSL ou quaisquer outras formas, nos equipamentos que estejam, ao mesmo tempo, conectados na rede local da Sociedade, salvo situações excepcionais aprovadas pelo Diretor de Compliance.

(ii) **Senhas**

- A senha é pessoal e intransferível, devendo obedecer aos padrões divulgados pela Sociedade. O Colaborador é responsável por todas as transações realizadas nos sistemas disponibilizados;
- A senha não deve, sob hipótese alguma, ser compartilhada com outras pessoas;
- O usuário não deve armazenar sua senha em arquivos de computador e tampouco escrevê-la em papéis ou outro tipo de mídia;
- As senhas de *logon* na rede devem estar de acordo com os seguintes aspectos:
  a) Conter no mínimo 06 (seis) caracteres;
  b) Possuir validade de no máximo 90 (noventa) dias;
  c) Possuir letras e números; e
  d) Devem ser criptografadas quando transmitidas ou armazenadas.

(iii) **Hardware e Software**

- Não é permitida a instalação e utilização de unidades de armazenamentos removíveis (pen drives, HDs externos, cartão de memória, mp3 e outros), salvo em casos autorizados pela Diretoria de Compliance.

(iv) **Alterações de Configuração**

- As configurações de hardware e software dos computadores disponibilizados pela Sociedade não devem ser alteradas. Caso haja necessidade de algum tipo de alteração, a Diretoria de Compliance deverá ser acionada através de solicitação por e-mail.

(v) **Internet**

- A Internet é uma ferramenta de trabalho utilizada pelos Colaboradores como apoio ao desenvolvimento de suas atividades e competências; e
- Não é permitido o acesso a e-mails pessoais e software de comunicação entre outros, caso necessário deverá ser solicitada autorização pelo gestor responsável à Diretoria de Compliance.

PROTEÇÃO CONTRA SOFTWARE MALICIOSO

8.2. O software de proteção contra vírus deve estar instalado e ativado em todos os computadores, e atualizado diariamente, não devendo, em nenhuma hipótese, ser desativado sem a autorização da área de TI. Caso o Colaborador identifique tal situação, deverá comunicar imediatamente o Diretor de Compliance, que tomará as medidas necessárias à correção do problema.

CÓPIA DE SEGURANÇA (BACKUP)

8.3. Cabe à área de TI realizar regularmente a cópia dos dados e informações mantidas nos equipamentos de armazenamento nos servidores da empresa.

8.4. Backup de e-mails armazenados nos computadores locais e móveis ingressados no domínio Sociedade será realizado diariamente.

TRATAMENTO DE MÍDIA

8.5. Não é permitido realizar cópia ou divulgar informações confidenciais para uso pessoal ou de terceiros. Tais cópias ou divulgações, quando necessárias, devem ser autorizadas pela Diretoria de Compliance.

TROCA DE INFORMAÇÕES

8.6. Uso do Correio Eletrônico (e-mail)

- A autorização de acesso ao correio eletrônico deve ser solicitada à área administrativa da Sociedade, que tomará as providências necessárias para tanto;
- O correio eletrônico é uma ferramenta de trabalho utilizada pelos Colaboradores como apoio ao desenvolvimento de suas atividades profissionais;
- Não é permitido utilizar o correio eletrônico para o envio de mensagens ou arquivos de conteúdo considerado impróprio pela Sociedade;
- É considerado impróprio o conteúdo que não está em conformidade com as regras legais, a moral, a integridade e os bons costumes, tais como campanhas políticas, religiosas, venda de produtos, boatos, jogos, músicas, filmes, vídeos e fotos que não esteja na conformidade do negócio;
- É proibido o download e envio de arquivos anexados ao e-mail com as extensões *.exe, *.pif, *.bat, *.com, *.scr, *.mp3, *.wav, *.wma, *.vbs, *.reg;
- Todos os e-mails do domínio serão armazenados pelo setor de TI, para auditorias internas e externas, e poderão ser consultados com a autorização da Diretoria de Compliance a qualquer momento sem prévio aviso; e
- Práticas recomendadas na utilização o e-mail:
    a) Envie e-mails apenas para os destinatários que realmente precisam da informação;
    b) Seja breve, pois assim, dificilmente as pessoas deixarão de ler a sua mensagem;
    c) Sempre que possível, não utilize anexos no e-mail; e
    d) Seja educado, não escreva nada que não diria pessoalmente.

8.7. Uso de Criptografia

- Somente é permitida a utilização de mecanismos de criptografia homologados pela Sociedade. Em caso de necessidades adicionais, a área de TI deverá ser acionada através de solicitação da área administrativa.

8.8. SOFTWARES E RECURSOS DE INFORMÁTICA

Instalação de Softwares

8.8.1. Somente é permitida a utilização de software devidamente homologado, licenciado, instalado e controlado pela área de TI.

Instalação e movimentação de Recursos de Informática

8.8.2. A instalação, controle, movimentação e manutenção de recursos computacionais de propriedade da Sociedade são de responsabilidade exclusiva da área de TI.

9. CONTROLE DE ACESSO:

9.1. Acesso Lógico

- Cada usuário de recursos computacionais da Sociedade deve possuir uma identificação (ID), a qual será utilizada como "conta de acesso" aos sistemas e redes da empresa;
- O cadastramento do usuário para o acesso aos recursos computacionais deve ser solicitado pela área administrativa à área de TI, a qual estabelecerá os perfis e autorizações de acesso;
- O usuário deve ter acesso somente às informações e recursos que forem necessários para a realização de suas atividades;
- As movimentações de pessoal (admissões, transferências, promoções, demissões, etc.) devem ser comunicadas pela área administrativa à área de TI, a fim de que as devidas atualizações nos ambientes computacionais sejam realizadas;

- Cabe ao gestor responsável por cada um dos contratos com fornecedores, quando do encerramento dos mesmos, solicitar por escrito à área administrativa o cancelamento dos acessos concedidos.

9.2. Desligamentos

- Será de responsabilidade da área administrativa informar os desligamentos de Colaboradores imediatamente para a área de TI, a qual realizará os bloqueios de acesso de imediato;
- O Colaborador deverá entregar todos os equipamentos de sua responsabilidade para a área de TI no momento de seu desligamento, como, por exemplo, celulares, notebooks, pen drives e outros, sob pena de restituição dos valores relativos a cada um dos equipamentos; e
- Dados de usuários desligados da Sociedade serão armazenados para utilização exclusiva da Sociedade e o e-mail redirecionado para o gestor da área. O Colaborador desligado não poderá realizar cópia de arquivos para sua utilização fora da empresa.

10. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

10.1. Qualquer violação a presente Política está sujeita a sansões disciplinares, observadas a natureza e gravidade da infração, conforme determinado pela Diretoria de Compliance.

10.2. Ao identificar ou suspeitar de possível violação das diretrizes estabelecidas nessa Política, o Colaborador Sociedade deve buscar orientação junto ao seu gestor ou ao Diretor de Compliance.