REIT
SECURITIZADORA

PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Esta Norma tem como objetivo definir responsabilidades e orientar a conduta dos profissionais e usuários de informática da REIT Securitizadora de Recebíveis imobiliários S.A. ("REIT") na utilização dos recursos computacionais, visando proteger a integridade e confidencialidade das informações.

Os recursos da tecnologia de informação disponibilizados pela REIT são destinados exclusivamente às atividades operacionais da instituição.

A REIT entende que o sistema de segurança adotado atingirá sua eficácia com o comprometimento e a cooperação de todos os profissionais envolvidos nos processos: colaboradores da REIT e Equipe de Tecnologia de Informação ("ETI").

Os programas homologados e instalados nos computadores e nos servidores de rede são propriedade exclusiva da REIT, sendo vedada sua cópia parcial ou integral.

2. DEFINIÇÕES

2.1. Segurança da Informação - diz respeito à proteção de determinados dados, com a intenção de preservar seus respectivos valores para uma organização (empresa) ou um indivíduo.
Podemos entender como informação todo o conteúdo ou dado valioso para um indivíduo/organização, que consiste em qualquer conteúdo com capacidade de armazenamento ou transferência, que serve a determinado propósito e que é de utilidade do ser humano.
Atualmente, a informação digital é um dos principais produtos de nossa era e necessita ser convenientemente protegida. A segurança de determinadas informações pode ser afetadas por vários fatores, como os comportamentais e do usuário, pelo ambiente/infraestrutura em que ela se encontra e por pessoas que têm o objetivo de roubar, destruir ou modificar essas informações.
Confidencialidade, disponibilidade e integridade são algumas das características básicas da segurança da informação, e podem ser consideradas até mesmo atributos.

2.2. Tecnologia da Informação - conjunto de todas as atividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações. Na verdade, as aplicações para TI são tantas — e estão ligadas a tantas áreas — que há diversas definições para a expressão e nenhuma delas consegue determiná-la por completo. É a área da informática que trata a informação, a organização e a classificação de forma a permitir a tomada de decisão em prol de algum objetivo. A tecnologia da informação pode contribuir para alargar ou reduzir as liberdades privadas e públicas ou tornar-se um instrumento de dominação.

TI refere-se, de modo geral, à coleção de recursos de informação de uma organização, seus usuários e a gerência que os supervisiona, inclusive a infraestrutura de TI e todos os outros sistemas de informação em uma organização.

1. RESPONSABILIDADES E COMPETÊNCIAS

1.1. Da Divisão de Tecnologia da Informação:

3.1.1. Zelar pelo cumprimento desta norma e notificar imediatamente a Diretoria de Compliance sobre quaisquer vulnerabilidades e ameaças de quebra de segurança;

3.1.2. Instalar ou remover componentes de tecnologia e sistemas de informação;

3.1.3. Fazer manutenção, controlar e homologar hardware e software de utilização da REIT;

3.1.4. Sugerir tecnicamente a aquisição de hardware e software necessários ao bom funcionamento das atividades da REIT;

3.1.5. Realizar auditorias de hardware e software a pedido da Diretoria de Compliance, com a finalidade de garantir a proteção dos recursos computacionais;

3.1.6. Sugerir a aquisição de serviços de informática necessários ao melhor funcionamento da REIT;

3.1.7. Criar e manter cópias de segurança (backups) dos dados de softwares críticos, armazenados nos servidores de redes;

3.1.8. Manter backups guardados em local seguro, separados dos equipamentos, para viabilizar a recuperação dos dados.

3.2. Da Diretoria de Compliance:

3.2.1. Definir e divulgar as medidas de Segurança da Informação;

3.2.2. Orientar e educar os funcionários sobre os preceitos atinentes à Segurança da Informação, bem como lhes assegurar treinamento para o uso correto dos recursos, visando evitar falhas e danos ao funcionamento dos sistemas informatizados;

3.2.3. Informar à Área de T.I. sobre acesso de novos usuários aos sistemas de informação, bem como atualizar nos sistemas as funções nas áreas de atuação;

3.2.4. Advertir formalmente e aplicar as sanções cabíveis quando o colaborador violar os princípios ou procedimentos de segurança;

3.2.5. Aprovar a solicitação de compra ou alteração de hardware e software, eventualmente indicados pela Área de T.I.

3.3. De todos os colaboradores:

3.3.1. Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para fins laborais;

3.3.2. Responder pelo uso exclusivo e intransferível de suas senhas de acesso;

3.3.3. Adquirir conhecimento técnico necessário para a correta utilização dos recursos de informática;

3.3.4. Relatar prontamente à Área de T.I. qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, vírus, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à Internet, programas instalados sem autorização, etc;

3.3.5. Assegurar que as informações e dados de propriedade da REIT não sejam disponibilizados a terceiros, a não ser com autorização por escrito;

3.3.6. Manter, obrigatoriamente, os dados críticos da empresa nos servidores de redes;

3.3.7. Relatar à Área de T.I. a possibilidade de instalação de um novo software ou aquisição de novo hardware para a melhoria dos serviços prestados.

2. REGRAS DE UTILIZAÇÃO DE CONTAS E SENHAS DA REDE CORPORATIVA

2.1. Todos os usuários da rede de dados corporativa da REIT receberão login e senha individual exclusivos para sua utilização. É importante que os usuários não utilizem senhas de fácil identificação, tais como: data de nascimento próprio ou de parentes próximos, nomes próprios, datas comemorativas nacionais ou pessoais, iniciais de nomes próprios, números de telefones e etc.

2.2. As senhas de acesso são pessoais, intransferíveis e não devem, em hipótese nenhuma, ser emprestadas ou compartilhadas com terceiros;

2.3. Não é permitida a utilização de computadores da rede sem senha ou com acesso local;

2.4. As senhas deverão ser alteradas pelo usuário, através de procedimento eletrônico e automático, utilizando o sistema de alteração de senhas disponível;

2.5. No caso do colaborador ser desligado da empresa, suas contas serão bloqueadas imediatamente, assim como suas senhas de acesso a qualquer recurso da rede ou sistemas;

2.6. Reserva-se a REIT o direito de auditar a utilização de contas de rede e sistemas fornecidos aos usuários de sua rede coorporativa, sem que se caracterize invasão de privacidade.

3. REGRAS PARA UTILIZAÇÃO DA REDE CORPORATIVA

3.1. Todos os recursos de rede de computadores deverão ser utilizados exclusivamente para fins profissionais, que envolvam atividades relacionadas ao bom andamento dos serviços e processos da REIT;

3.2. Todos os computadores da REIT devem ter antivírus instalado e atualizado periodicamente, é proibido desinstalar e utilizar computadores sem antivírus instalado;

3.3. É expressamente vedado aos usuários a instalação ou remoção de programas de computador, componente e periféricos sem prévia autorização e ciência da Área de T.I.;

3.4. É proibido aos usuários conectar computadores pessoais ou de terceiros à rede coorporativa da REIT, exceto a utilização de notebooks e outros equipamentos portáteis através da rede sem fio "WiFi".

4. REGRAS PARA UTILIZAÇÃO DO CORREIO ELETRÔNICO (E-MAIL)

4.1. A REIT fornecerá, a seu critério, contas de correio eletrônico aos seus colaboradores. As mensagens de correio eletrônico (e-mails) internos e externos devem ser exclusivamente de caráter profissional, sendo proibido qualquer tipo de utilização particular. O mesmo vale para arquivos anexos;

4.2. É proibido configurar e/ou manter configuradas contas de correio eletrônico de servidores externos, isto é, diferentes das oferecidas pela Área de T.I., nos programas gerenciadores de correio eletrônico instalados em computadores da REIT;

4.3. O conteúdo das mensagens enviadas através de contas de correio da REIT é de inteira responsabilidade do usuário que utiliza a conta e que possui a senha com acesso exclusivo à caixa postal e para envio de mensagens;

4.4. É proibida a utilização do e-mail corporativo para fins ilegais, transmissão de material de qualquer forma censurável, que viole direitos de terceiros e leis aplicáveis;

4.5. É proibida a utilização de e-mail para transmitir mensagens conhecidas como Spam, JunkMail, correntes ou a distribuição de mensagens em massa não solicitadas;

4.6. É terminantemente proibido aos representantes da Área de T.I., administradores de rede e/ou correio eletrônico, ler mensagens de correio eletrônico de qualquer usuário quando estiver realizando serviços de manutenção e suporte, exceto quando em cumprimento de determinações da Diretoria da REIT para efeitos de auditoria;

4.7. Reserva-se a REIT o direito de auditar a utilização de suas contas de correio eletrônico fornecidas aos usuários, sem que se caracterize invasão de privacidade.

5. REGRAS PARA UTILIZAÇÃO DA INTERNET

5.1. O acesso à Internet é disponibilizado aos colaboradores da REIT para viabilizar a busca de informações ou agilizar determinados processos exclusivamente necessários ao desenvolvimento dos trabalhos necessários à instituição;

5.2. Os usuários são responsáveis pela utilização da Internet em computadores acessados com seu login e senha. Ao se afastar do computador, o colaborador deverá encerrar a sessão através de "logoff", reiniciar ou desligar o sistema;

5.3. É proibido aos usuários configurar ou alterar as configurações de rede e de acesso à Internet dos computadores da REIT, incluindo as seguintes configurações de rede: IP, DNS, WINS, Gateway, Proxy e a instalação ou reconfiguração de clientes Proxy;

5.4. Não é permitido enviar, baixar (download) ou manter arquivos de imagens, musicas, vídeo, arquivos executáveis em geral ou quaisquer outros de caráter pessoal nas estações de trabalho da REIT;

5.5. É proibido o acesso a sites de relacionamento em geral, como Facebook, Twitter, e outros, a não ser para assuntos exclusivos ao desenvolvimento de atividades necessárias à REIT;

5.6. Não é permitido o acesso a sites de Internet com conteúdo pornográfico, jogos, bate-papo, chat, blogger, cartoon, relacionamento, música, hacker ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia, senhas ou outros eventos de segurança;

5.7. É proibido o acesso a sites, a instalação e a utilização de programas de troca de mensagens instantâneas ou arquivos do tipo: Facebook Messenger, ICQ, MSN Messenger, Yahoo Messenger, Bittorrent, Imesh, AudioGalaxy, AIM, Morpheus, Kaaza, Emule, Napster e outros;

5.8. Sempre que os usuários, utilizando o Internet, tiverem acesso a materiais criminosos como pornografia infantil (arte, textos, figuras, cenas, imagens) e outros, mesmo que de maneira esporádica e involuntária, deverão entrar em contato imediatamente com a Área de T.I. e/ou com a Diretoria de Compliance para relatar o fato ocorrido.

6. REGRAS PARA UTILIZAÇÃO DA REDE SEM FIO (WIFI)

6.1. Usuários autorizados poderão conectar computadores ou outros equipamentos portáteis e pessoais a Internet, utilizando a rede sem fio ("WiFi") da REIT.

6.2. O acesso à internet através da rede WiFi poderá ser controlado com a realização de auditorias nas páginas consultadas à critério da REIT.

6.3. Os usuários são responsáveis pela utilização da internet através da rede WiFi da REIT, e serão identificados e responsabilizados em caso de acesso indevido.

7. PENALIDADES

7.1. A REIT alerta todos os usuários que a instalação ou utilização de software não autorizados constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena de detenção e multa.

7.2. Todos os usuários são responsáveis pelo uso correto das ferramentas eletrônicas disponibilizadas.

7.3. Todas as práticas que representam ameaça à segurança da informação serão tratadas com a aplicação de ações disciplinares.

7.4. Portanto, na ocorrência de infrações a esta Norma ou às determinações constantes de comunicações externas ou internas, ou mesmo às ordens de superiores hierárquicos, quando for o caso, ficam os infratores sujeitos às seguintes penalidades: advertência verbal, advertência por escrito, suspensão, demissão sem ou com justa causa e/ou outras medidas judiciais cabíveis;

7.5. Todos os usuários passam ter acesso a este manual, dando ciência de seu conteúdo. Os novos colaboradores/usuários terão acesso ao mesmo material por ocasião de sua admissão na REIT e deverão assinar o "Termo de Adesão às Políticas Internas – TAPI".

7.6. As decisões de medidas a serem adotadas quanto aos casos não tratados nesta Norma serão de responsabilidade da Diretoria de Compliance.