Política de Segurança

Documento de Diretrizes e Normas Administrativas

Elaborado pelo comitê gestor da empresa – Vigente 2014

Sumário

1. INTRODUÇÃO

A segurança é um dos assuntos mais importantes dentre as preocupações de qualquer empresa.

Nesse documento apresentaremos um conjunto de instruções e procedimentos para normatizar e melhorar nossa visão e atuação em segurança.

Todo e qualquer usuário da companhia tem a responsabilidade de proteger a segurança e a integridade das informações.

1.1. A empresa e a política de segurança

Todas as normas aqui estabelecidas serão seguidas à risca por todos os funcionários, parceiros e prestadores de serviços. Ao receber essa cópia da Política de Segurança, o/a Sr./Sra. comprometeu-se a respeitar todos os tópicos aqui abordados e está ciente de que seus e-mails e navegação na internet/intranet podem estar sendo monitorados. A equipe de segurança encontra-se a total disposição para saneamento de dúvidas e auxílio técnico.

1.2. O não cumprimento desta política

A violação desta política de segurança é qualquer ato que:

- Exponha a Companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.

- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

2. CLASSIFICAÇÃO DAS INFORMAÇÕES

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

1 – Pública

2 – Interna

3 – Confidencial

4 – Restrita

Conceitos:

Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

3. DADOS PESSOAIS DE FUNCIONÁRIOS

A SUNDELL se compromete em não acumular ou manter intencionalmente dados pessoais de funcionários além daqueles relevantes na condução do seu negócio.

Todos os dados pessoais de funcionários serão considerados dados confidenciais.

Dados pessoais de funcionários sob a responsabilidade da SUNDELL não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados pessoais de funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da SUNDELL.

4. SOFTWARES ILEGAIS

É terminantemente proibido o uso de programas ilegais (PIRATAS) na SUNDELL. Os usuários não podem, em hipótese alguma, instalar este tipo de *software* (programa) nos equipamentos da Companhia.

Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

5. AUTENTICAÇÃO

A autenticação nos sistemas de informática serão baseados em uma senha. Esse meio é muito utilizado por sua facilidade de implantação e manutenção e por seu baixo custo. Infelizmente esse meio também é o mais inseguro.

Senhas como nome do usuário, combinações simples (abc123), substantivos (casa, meia, cadeira, brasil), datas (11092001) e outros são extremamente fáceis de descobrir. Então aprenda a criar senha de forma coerente, observando nossa política de senhas.

5.1 Política de Senhas

Uma senha segura deverá conter no mínimo 6 caracteres alfanuméricos (letras e números) com diferentes caixas.

Para facilitar a memorização das senhas, utilize padrões de fácil memorização. Por exemplo:

eSus6C (eu SEMPRE uso seis 6 CARACTERES)

odIamp0709 (ouviram do Ipiranga as margens plácidas 7 de Setembro)

s3Nh45 (A palavra senha onde o 3 substitui o E, o 4 o A e o 5 o S)

As senhas terão um tempo de vida útil determinado pela equipe de segurança, devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso aos sistemas.

- Sua senha não deve ser jamais passada a ninguém, nem mesmo da equipe de segurança. Caso desconfie que sua senha não está mais segura, sinta-se à vontade para alterá-la, mesmo antes do prazo determinado de validade;

- Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para manter sua senha secreta.

5.2 Política de e-mail

- Não abra anexos com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza absoluta de que solicitou esse e-mail;

- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês;

- Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc;

- Não utilize o e-mail da empresa para assuntos pessoais;

- Não mande e-mails para mais de 10 pessoas de uma única vez (to, cc, bcc);

- Evite anexos muito grandes;

- Utilize sempre sua assinatura criptográfica para troca interna de e-mails e quando necessário para os e-mails externos também.

5.3 Políticas de acesso à Internet

- O uso recreativo da internet não deverá se dar no horário de expediente;

- Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de segurança com prévia autorização do supervisor do departamento local;

- Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado;

- É proibido o uso de ferramentas P2P (kazaa, Morpheus, etc);

- É proibido o uso de IM (Instant messengers) não homologados/autorizados pela equipe de segurança.

Lembrando novamente que o uso da internet estará sendo auditado constantemente e o usuário poderá vir a prestar contas de seu uso.

6. CÓPIAS DE SEGURANÇA DE ARQUIVOS INDIVIDUAIS

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da SUNDELL.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da SUNDELL o Setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

7. TRANSFERÊNCIA DE ARQUIVOS

Quando um funcionário for promovido ou transferido de seção ou gerência, o setor de cargos e salários deverá comunicar o fato ao Setor de Informática, para que sejam feitas as adequações necessárias para o acesso do referido funcionário ao sistema informatizado da Companhia.

8. COMPARTILHAMENTO DE PASTAS E DADOS

É de obrigação dos usuários rever periodicamente todos os compartilhamentos existentes em suas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos.

9. USO DE ANTIVÍRUS

Todo arquivo em mídia proveniente de entidade externa deve ser verificado por programa antivírus.

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.

Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

10. PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

11. DISPOSIÇÕES FINAIS

Fica estabelecida a obrigatoriedade, a todos os atuais e novos funcionários e colaboradores, da assinatura do termo de conhecimento à Política de Segurança da empresa.