Universidade Federal Rural de Pernambuco
Segurança e Auditoria de Sistemas de Informação
Edson Fagner da Silva Cristovam

Política de uso aceitável

Objetivo

O objetivo desta política é descrever o uso aceitável de equipamentos de informática na empresa. Essas regras existem para proteger o funcionário e a empresa.

O uso impróprio expõe a empresa a riscos, incluindo ataques de vírus, comprometimento de sistemas e serviços de rede, além de questões legais.

Escopo

Esta política se aplica ao uso de informações, dispositivos eletrônicos e de computação e recursos de rede para conduzir negócios da empresa ou interagir com redes internas e sistemas de negócios, sejam de propriedade ou alugados por empresa, funcionário ou um terceiro.

Todos os funcionários, consultores e temporários são responsáveis por exercer o bom senso em relação ao uso adequado de informações, dispositivos eletrônicos e recursos de rede.

Políticas

Uso geral e propriedade

1. Informações proprietárias da empresa armazenadas em dispositivos eletrônicos e de computação, se pertencente ou alugado pela empresa, o funcionário ou um terceiro, permanece como propriedade exclusiva da empresa. Você deve garantir, por meios legais ou técnicos, que as informações proprietárias sejam protegidas.
2. Você tem a responsabilidade de relatar imediatamente o roubo, perda ou divulgação não autorizada de informações proprietárias da empresa.
3. Você pode acessar, usar ou compartilhar informações proprietárias da empresa somente na medida em que for autorizado e necessário para cumprir suas funções atribuídas.
4. Para fins de segurança e manutenção de rede, indivíduos autorizados na empresa podem monitorar equipamentos, sistemas e tráfego de rede a qualquer momento.

Segurança e informações proprietárias

1. Todos os dispositivos móveis e de computação que se conectam à rede interna devem cumprir a “Política de Acesso Mínimo”.

2. As senhas de nível de sistema e de usuário devem estar em conformidade com a Política de Senha. É proibido fornecer acesso a outro indivíduo, deliberadamente ou por meio da falha em proteger seu acesso.
3. Todos os dispositivos de computação devem ser protegidos por uma proteção de tela e por senha com o recurso de ativação automática definido em no máximo 10 minutos. Você deve bloquear a tela ou fazer logoff quando o dispositivo estiver sem sua supervisão.
4. Os funcionários devem ter muito cuidado ao abrir anexos de e-mail recebidos de remetentes desconhecidos, que podem conter malware.

Uso inaceitável

1. Sob nenhuma circunstância um funcionário da empresa está autorizado a se envolver em qualquer atividade que seja ilegal sob as leis locais, estaduais, federais ou internacionais enquanto utiliza recursos de propriedade da empresa.
2. É proibido acessar dados, um servidor ou uma conta para qualquer finalidade que não seja a condução dos negócios da empresa, mesmo se você tiver acesso autorizado.
3. Introdução de programas maliciosos na rede ou servidor (por exemplo, vírus, worms, cavalos de Tróia, etc.).
4. Revelar a senha da sua conta a terceiros ou permitir o uso da sua conta por terceiros. Isso inclui a família e outros membros da família quando o trabalho está sendo feito em casa.
5. Executar qualquer forma de monitoramento de rede que interceptará dados não destinados ao host do funcionário, a menos que essa atividade faça parte do trabalho ou dever do funcionário.
6. Fornecimento de informações da empresa para terceiros fora da empresa.

Política de acesso remoto

Objetivo

O objetivo desta política é definir regras e requisitos para se conectar à rede da empresa a partir de qualquer host. Essas regras e os requisitos são projetados para minimizar a exposição potencial da empresa a danos que podem resultar do uso não autorizado dos recursos da empresa.

Os danos incluem a perda de dados sensíveis ou confidenciais da empresa, propriedade intelectual, danos à imagem pública, danos aos sistemas internos críticos da empresa e multas ou outras responsabilidades financeiras incorridas como resultado dessas perdas.

Escopo

Esta política se aplica a todos os funcionários, fornecedores e agentes da empresa com um computador ou estação de trabalho de propriedade da empresa ou pessoal usado para se conectar à rede da empresa.

Esta política se aplica a conexões de acesso remoto usadas para trabalhar em nome da empresa, incluindo leitura ou envio de e-mail e visualização de recursos da intranet da web.

Esta política cobre toda e qualquer implementação técnica de acesso remoto usado para conectar-se às redes da empresa.

Políticas

É responsabilidade dos funcionários, fornecedores e agentes da empresa com privilégios de acesso remoto à rede corporativa da empresa garantir que sua conexão de acesso remoto receba a mesma consideração que a conexão do usuário no local de trabalho na empresa.

Ao acessar a rede da empresa de um computador pessoal, os usuários autorizados são responsáveis por impedir o acesso a quaisquer recursos ou dados do computador da empresa por usuários não autorizados.

É proibida a realização de atividades ilegais por meio da rede da empresa por qualquer usuário (autorizado ou não). O usuário autorizado assume a responsabilidade e as consequências do uso indevido do acesso do usuário autorizado.

Requisitos

1. O acesso remoto seguro deve ser estritamente controlado com criptografia e redes privadas virtuais (VPNs) e frases secretas fortes.
2. Os usuários autorizados deverão proteger seu login e senha, inclusive de familiares.
3. Ao usar um computador de propriedade da empresa para se conectar remotamente à rede corporativa, os usuários autorizados devem garantir que o host remoto não esteja

conectado a qualquer outra rede ao mesmo tempo, com exceção das redes pessoais que estão sob seu controle total ou sob o controle total de um usuário autorizado.

4. O uso de recursos externos para conduzir os negócios da empresa deve ser aprovado com antecedência pelo gerente da unidade de negócios apropriado.
5. O equipamento pessoal usado para se conectar às redes da empresa deve atender aos requisitos para acesso remoto, conforme declarado nos padrões de configuração de hardware e software para acesso remoto às redes da empresa.

Política de Email

Objetivo

O objetivo desta política de e-mail é garantir o uso adequado do sistema de e-mail da empresa e conscientizar os usuários sobre o que a empresa considera o uso aceitável e inaceitável de seu sistema de e-mail.

Esta política descreve os requisitos mínimos para o uso de e-mail na rede da empresa.

Escopo

Esta política cobre o uso apropriado de qualquer e-mail enviado de um endereço de e-mail da empresa e se aplica a todos os funcionários, fornecedores e agentes que operam em nome da empresa.

Política

1. Todo uso de e-mail deve ser consistente com as políticas e procedimentos da empresa de conduta ética, segurança, conformidade com as leis aplicáveis e práticas comerciais adequadas.
2. A conta de e-mail da empresa deve ser usada principalmente para fins comerciais da empresa; comunicação pessoal é permitida de forma limitada, mas usos comerciais não relacionados à empresa são proibidos.
3. Todos os dados da empresa contidos em uma mensagem de e-mail ou anexo devem ser protegidos de acordo com o padrão de proteção de dados.
4. O sistema de e-mail da empresa não deve ser usado para a criação ou distribuição de qualquer mensagem ofensiva, incluindo comentários ofensivos sobre raça, sexo, cor de cabelo, deficiência, idade, orientação sexual, pornografia, crenças e práticas religiosas ou nacionalidade.
5. Os funcionários que receberem e-mails ofensivos de qualquer funcionário da empresa devem relatar o assunto ao seu supervisor imediatamente.
6. Os usuários estão proibidos de usar sistemas de e-mail e servidores de terceiros para conduzir negócios da empresa, criar ou memorizar quaisquer transações vinculativas ou armazenar ou reter e-mail em nome de empresa. Essas comunicações e transações devem ser conduzidas por meio dos canais apropriados, descritos na documentação aprovada pela empresa.
7. O uso de uma quantidade razoável de recursos da empresa para e-mails pessoais é aceitável, mas os e-mails não relacionados ao trabalho devem ser salvos em uma pasta separada do e-mail relacionado ao trabalho.
8. Os funcionários da empresa não devem ter expectativa de privacidade em nada que armazenem, enviem ou recebam no sistema de e-mail da empresa.
9. A empresa pode monitorar e-mails sem aviso prévio.