❖ 22.2 – Controle de Segurança Cibernético

❖ *22.2.1 – Controle de Riscos*

PROPIEDADE DA INFORMAÇÃO, DADOS E SOFTWARES

Definições

Informação: Conhecimento, de todas as formas que geram valor para a empresa

Dados: Qualquer informação dentro do computador, incluindo e não limitado a informações inseridas, armazenadas ou recuperadas de um computador. Exemplos incluem planilhas e dados inseridos.

Software: Sistema operacional do Computador e programas

Política de Procedimento

Todas as informações e dados gerados ou coletados por um usuário, no curso de seu emprego na Empresa e/ou utilizando ativos de propriedade da Empresa, serão propriedade exclusiva da Empresa. Nenhuma informação ou dado será transferido, dado ou emprestado a qualquer organização ou indivíduo externo, exceto para aquelas instâncias em que estiver no curso aprovado de negócios para a Empresa e com a autorização expressa por escrito de um gerente autorizado.

Todo software comprado, licenciado ou criado pela Empresa é propriedade exclusiva da Empresa e não pode ser transferido, dado ou emprestado a nenhuma outra organização ou indivíduo externo sem a autorização expressa por escrito do Gerente Geral. Da mesma forma, tal software não pode ser instalado em computadores de propriedade pessoal sem a autorização expressa por escrito do Gerente Geral.

A violação desta política resultará em ação disciplinar até e incluindo demissão

SEGURANÇA DA INFORMAÇÃO

Definições

Informações sensíveis, confidenciais ou de qualquer natureza que a empresa usa para sua vantagem e negócios, isso inclui: Listagem de clientes, funcionários, projetos, planos de negócio, informações de pesquisa e desenvolvimento, vendas, contratos pendentes, custos de produção e serviço, informações financeiras.

Política de Procedimento

Um método comum para obter acesso a redes de computadores é um hacker se passar por um membro do departamento de TI de uma empresa. Por exemplo, um hacker ligará para um funcionário com uma história de que precisa do ID de login e senha do funcionário. Uma vez que os hackers os tenham, eles estarão a caminho de invadir a rede. O pessoal de TI da Transworld nunca ligará para os funcionários e pedirá seu ID de login e/ou senha. Os funcionários não devem divulgar seus IDs de login ou senha a ninguém além do Gerente Geral.

As senhas devem ter no mínimo (06) caracteres e conter letras e números. Palavras, nomes, datas de nascimento, endereços, códigos postais, números de telefone, números de previdência social ou qualquer outra combinação facilmente adivinhada não podem ser usados. IDs de usuário e/ou senhas não podem ser anotados e mantidos dentro da área geral do computador. Os usuários não podem utilizar senhas internas ou senhas substancialmente semelhantes em sistemas externos (por exemplo: sites, e-mail baseado na web, etc.).

Os usuários não podem permitir que nenhuma pessoa acesse, de nenhuma maneira, seu equipamento de computador designado, a menos que essa pessoa esteja especificamente autorizada a fazê-lo.

A perda de qualquer equipamento de computador ou qualquer informação da Empresa deve ser imediatamente reportada ao Gerente Geral ou Gerente de TI,

que garantirá imediatamente que todas as medidas possíveis sejam tomadas para proteger a Empresa de mais perda de informações.

Qualquer tentativa de outra pessoa de obter um ID de login e/ou senha, ou qualquer outra atividade suspeita, deve ser reportada ao Gerente Geral.

Todas as informações criadas, obtidas ou utilizadas pelos usuários no curso de seu emprego são propriedade exclusiva da Empresa. Mesmo quando fisicamente capazes, os usuários não acessarão nenhuma informação além daquela que eles estão especificamente autorizados a acessar e são necessárias para o desempenho de suas tarefas atribuídas. As informações da Empresa não podem ser utilizadas para o benefício de nenhuma outra pessoa ou organização.

A menos que especificamente designado de outra forma, todas as informações são consideradas confidenciais. As informações que são um Segredo Comercial, sensíveis ou confidenciais nunca serão disseminadas, por qualquer meio, para pessoas fora da Empresa, a menos que todas as seguintes condições sejam atendidas:

1. A disseminação é expressamente aprovada, com antecedência, por um gerente autorizado

2. As informações de Segredo Comercial, Sensíveis ou Confidenciais são:

    A: Criptografado, se for um arquivo de computador, caso contrário

    B: Selado em um envelope ou outro recipiente apropriado

3. O texto da carta de transmissão ou e-mail inclui um aviso ao destinatário de que o material é segredo comercial, sensível ou confidencial e é propriedade da empresa

4. O texto da carta de transmissão ou e-mail inclui uma declaração específica do destinatário que o está recebendo, o que ele/ela está autorizado/a a fazer com as informações e a quem, se houver, ele/ela pode divulgá-las

5. Uma cópia da carta de transmissão ou e-mail é arquivada permanentemente pelo usuário

Todos os usuários garantirão que qualquer material a ser descartado que contenha informações de segredo comercial, sensível ou confidencial, no todo ou em parte, será destruído de forma adequada e imediata.

Todos os usuários garantirão que qualquer informação de segredo comercial, sensível ou confidencial será retirada das instalações da empresa somente para fins comerciais permitidos e será criptografada usando software de criptografia aprovado com a senha arquivada com o gerente geral.

Todos os computadores terão software antivírus e antispyware instalado. Este software deve permanecer ativado o tempo todo. O gerente de TI garantirá que o software seja atualizado conforme apropriado.

A violação desta política resultará em ação disciplinar, incluindo demissão.

ACESSO DA EMPRESA AS INFORMAÇÕES DO COMPUTADOR E HARDWARE

Política de Procedimento

Todos os recursos relacionados a computadores sob o controle da Empresa existem para o avanço das atividades comerciais da Empresa. A Empresa pode inspecionar ou monitorar qualquer computador, dispositivo de computador, rede, instalação de computador ou dispositivo de armazenamento de propriedade da empresa, alugado ou controlado a qualquer momento e por qualquer motivo. Isso inclui a inspeção de e-mail (recebido, enviado ou armazenado) e o monitoramento para qualquer parte que considere apropriado.

O uso de criptografia, a rotulagem de um e-mail ou documento como privado, a exclusão de um e-mail ou documento ou qualquer outro processo ou ação não diminuirá os direitos da Empresa de nenhuma maneira.

Somente criptografia autorizada pela Empresa pode ser utilizada. Todas as senhas/chaves de criptografia devem estar arquivadas com o Gerente Geral antes de sua utilização.

A violação desta política resultará em ação disciplinar até e incluindo demissão.

INSTALAÇÃO E USO DE SOFTWARES

Definições

Pirataria de software: Pirataria de software é utilizar software em violação ao seu contrato de licenciamento.

Software: Qualquer programa de computador, incluindo plug-ins de navegador da web, complementos e barras de ferramentas.

Política de Procedimento

Sem a autorização prévia por escrito do Gerente Geral ou de TI, o usuário não deve:

1) Instalar nenhum software em equipamentos de informática de propriedade da empresa.

2) Instalar software de propriedade da empresa em qualquer equipamento de informática que não seja de propriedade da empresa

3) Fornecer cópias de software de propriedade da empresa ou licenciado a qualquer pessoa. Os usuários não se envolverão em nenhum ato de pirataria de software.

O Gerente de TI deve garantir que todo software instalado ou utilizado em máquinas da empresa esteja devidamente licenciado.

A violação desta política resultará em ação disciplinar até e incluindo demissão.

USO PESSOAL DO COMPUTADOR E SOFTWARE

Política de Procedimento

O hardware e software de computador de propriedade da empresa só podem ser utilizados para fins comerciais relacionados à empresa. Nenhum uso pessoal de ativos da empresa é permitido; isso inclui o sistema de e-mail da empresa e o acesso à Internet.

Tal uso não deve incluir:

1) Atividade política

2) Pornografia

3) Material sexista

4) Material racial

5) Qualquer ato ilegal

6) Assédio a um indivíduo ou organização

7) Busca de um companheiro

8) Qualquer outro comportamento inapropriado

A violação desta política resultará em ação disciplinar até e incluindo demissão.

EMAIL ELETRONICO

Definições

Sistema de e-mail: todos os meios de envio e recebimento de e-mail eletrônico (e-mail), incluindo e-mail interno e e-mail da internet.

Segredo comercial, Sensível ou Confidencial: qualquer informação, em qualquer formato, que seja uma vantagem comercial para a Empresa de qualquer forma. Isso inclui: listas de clientes/consumidores, listas de funcionários, projeções de negócios, planos de negócios, processos proprietários, informações sobre pesquisa e desenvolvimento, vendas pendentes, compras pendentes, contratos pendentes, custos de produção, cronogramas de produção, desenhos de design e informações financeiras da empresa.

Política de Procedimento

Esta política se aplica a qualquer pessoa que tenha acesso aos sistemas de e-mail da Empresa.

O sistema de e-mail da Empresa deve ser usado apenas para fins comerciais; nenhum uso pessoal do sistema de e-mail é permitido.

Todos os e-mails criados, enviados ou recebidos por meio dos computadores, redes e/ou sistemas de e-mail da Empresa são de propriedade da Empresa.

A Empresa reserva-se o direito de monitorar e/ou revisar, a qualquer momento, qualquer e-mail criado, enviado ou recebido por meio dos computadores, redes e/ou sistemas de e-mail da Empresa. A Empresa reserva-se ainda o direito de revelar o conteúdo de tal e-mail a qualquer parte que considere apropriada. O uso de criptografia, a rotulagem de um e-mail como privado, a exclusão de um e-mail ou qualquer processo ou ação desse tipo não diminuirá os direitos da Empresa de nenhuma maneira.

A Empresa divulgará o e-mail a qualquer parte que seja obrigada por lei ou regulamento. Isso pode incluir divulgação de acordo com mandados de busca e solicitações de descoberta de autoridades policiais em litígios civis.

Embora um usuário possa excluir uma mensagem de e-mail, cópias do e-mail ainda podem permanecer em servidores e fitas de backup.

Somente a criptografia autorizada pela Empresa pode ser utilizada. Todas as senhas/chaves de criptografia devem estar arquivadas com o Gerente Geral ou um fornecedor de TI designado antes de sua utilização.

Todos os e-mails endereçados a qualquer pessoa(s) fora da Empresa terão um aviso padrão na parte inferior do texto, declarando " Aviso: Esta mensagem (incluindo qualquer arquivos transmitidos juntos) é destinada exclusivamente para a(s) pessoa(s) a quem é dirigida, podendo conter informação confidencial e legalmente protegida. Se você não for destinatário desta mensagem, desde já fica notificado de abster-se a divulgar, copiar, distribuir, examinar ou, de qualquer forma, utilizar a informação contida nesta mensagem, por ser ilegal. Caso você não seja o destinatário, pedimos que responda essa mensagem informando o acontecido e delete todos as copias deste email de seu sistema.". Isso não se aplica a e-mails escritos por usuários que estão autorizados a entrar em acordos em nome da Empresa quando o e-mail fizer parte de um curso de negócios autorizado.

Todos os e-mails endereçados a qualquer pessoa(s) fora da Empresa identificarão claramente o funcionário que enviou o e-mail pelo nome completo e cargo oficial. O número de telefone do funcionário será incluído.

Os funcionários não se inscreverão em nenhuma lista de e-mail que não seja diretamente relevante para suas funções atribuídas.

Devido ao risco potencial de violações de segurança, os funcionários devem ter extremo cuidado ao baixar e executar quaisquer arquivos anexados ao e-mail. Se o anexo não for claramente relacionado aos negócios e/ou esperado de uma fonte conhecida, ele nunca deve ser aberto ou executado. Esses e-mails e anexos devem ser imediatamente encaminhados ao Gerente Geral ou Gerente de TI.

Informações que sejam um Segredo Comercial, Sensível ou Confidencial nunca serão enviadas por e-mail para pessoas fora da Empresa, a menos que todas as seguintes condições sejam atendidas:

1) A transmissão do e-mail seja expressamente aprovada, com antecedência, por um gerente autorizado

2) As informações de segredo comercial, sensíveis ou confidenciais sejam criptografadas

3) O texto do e-mail inclui um aviso ao destinatário de que o material é Segredo Comercial, sensível ou Confidencial e propriedade da Empresa

4) O texto do e-mail contém uma declaração específica do motivo pelo qual o destinatário o está recebendo, o que ele pode fazer com as informações e a quem, se houver, ele pode divulgá-las

5) Uma cópia do e-mail é arquivada permanentemente pelo usuário

Cada funcionário é responsável por garantir que seu uso do sistema de e-mail da Empresa seja consistente com esta política, qualquer outra política aplicável da Empresa e práticas comerciais apropriadas. Os e-mails não devem conter piadas, pornografia, comentários sexistas, comentários racistas, comentários difamatórios, comentários obscenos, qualquer coisa de natureza comercial não pertinente aos negócios da Empresa, qualquer coisa de natureza política ou quaisquer outros comentários inapropriados. Além disso, o sistema de e-mail não deve ser usado para qualquer propósito que viole a lei ou regulamento.

O sistema de e-mail da Empresa não será utilizado pelos usuários para nenhuma atividade comercial ou não comercial que não seja em prol dos negócios da Empresa. A atividade proibida inclui solicitação de contribuições de caridade e vendas de produtos de um usuário para outro. E-mails de "cartas em cadeia" não serão criados ou encaminhados.

Os usuários revisarão cuidadosamente todos os e-mails antes de enviá-los para garantir que seu significado seja claro e não sujeito a interpretação. Humor e sarcasmo podem ser facilmente mal interpretados em um e-mail e devem ser evitados. As mensagens de e-mail devem ser compostas de maneira profissional.

Comentários que seriam inapropriados em memorandos e cartas são igualmente inapropriados em e-mails.

Além daqueles especificamente atribuídos ou aprovados pelo Gerente Geral ou um fornecedor de TI designado, a utilização de ativos de computador de propriedade da empresa para acessar qualquer conta de e-mail ou serviço por um usuário é expressamente proibida; isso inclui serviços de e-mail como AOL, Hotmail, Gmail e qualquer outro serviço.

Os usuários não revelarão suas senhas de e-mail a ninguém. Excluindo membros da Gerência e fornecedores de TI designados, no curso de suas tarefas atribuídas, os usuários não utilizarão ou acessarão contas de e-mail pertencentes a nenhum outro usuário.

A violação desta política resultará em ação disciplinar até e incluindo demissão.

USO DA INTERNET

Política de Procedimento

Esta política se aplica a qualquer pessoa que utilize os sistemas de acesso à Internet da Empresa.

O acesso à Internet da Empresa deve ser usado apenas para fins comerciais; nenhum uso pessoal do acesso à Internet é permitido.

Todas as informações criadas, enviadas ou recebidas por meio dos computadores, redes, acesso à Internet e/ou sistema de e-mail da Empresa são de propriedade da Empresa.

A Empresa reserva-se o direito de monitorar, filtrar e/ou revisar, a qualquer momento, toda a utilização da Internet por meio do acesso à Internet da Empresa. A Empresa também reserva-se o direito de revelar qualquer informação relacionada ao acesso à Internet a qualquer parte que considere apropriada. O uso de criptografia, a rotulagem de uma comunicação como privada, a exclusão de uma comunicação ou qualquer processo ou ação desse tipo não diminuirá o direito da empresa de nenhuma maneira.

A Empresa divulgará informações de acesso à Internet a qualquer parte que seja obrigada por lei ou regulamento. Isso pode incluir mandados de busca e solicitações de descoberta em litígios civis.

Os usuários não acessarão nenhum material que não seja diretamente relevante para suas funções atribuídas.

Devido ao potencial risco de violações de segurança, os usuários não baixarão software da Internet, a menos que tenham obtido aprovação prévia por escrito do Gerente Geral ou de um fornecedor de TI designado. Isso inclui complementos de navegador da Web ou outros softwares que forneçam barras de pesquisa, clima, protetores de tela, etc.

Cada usuário é responsável por garantir que seu uso do acesso à Internet da Empresa seja consistente com esta política, qualquer outra política aplicável da Empresa e práticas comerciais apropriadas. Sites da Internet que contenham piadas, pornografia, material sexista, material racista, material difamatório, material obsceno, software pirateado, anúncios pessoais ou qualquer outro material inapropriado não devem ser acessados. Além disso, o sistema de acesso à Internet não deve ser usado para nenhuma finalidade que viole a lei ou regulamentação.

O acesso à Internet da Empresa não será utilizado para nenhuma atividade comercial ou não comercial que não seja em prol dos negócios da Empresa.

Os usuários devem estar cientes de que os sites da Internet que visitam coletam informações sobre os visitantes. Essas informações vincularão o usuário à Empresa. Os usuários não visitarão nenhum site que possa de alguma forma causar danos à imagem ou reputação da Empresa.

Os usuários devem estar cientes de que muito do material disponível na Internet é protegido por direitos autorais ou marca registrada. Além de visualizar material disponível publicamente, os usuários não usarão nenhum material encontrado na Internet de nenhuma maneira sem primeiro estabelecer que tal uso não violaria direitos autorais ou marca registrada.

Sem autorização prévia por escrito do Gerente Geral, os usuários não postarão comentários ou declarações em nenhuma página da Web ou enviarão mensagens para grupos de notícias da Internet.

Os usuários não entrarão em nenhuma sala de bate-papo ou canal de bate-papo da Internet.

Além daqueles especificamente aprovados pelo Gerente Geral ou um fornecedor de TI designado, a utilização de chat de bate-papo com clientes baseados na Internet (mensagens instantâneas whatsapp, MSN Messenger, ICQ, etc.) é expressamente proibido. Quando aprovado, o software de bate-papo será usado apenas para comunicações comerciais.

Devido ao esgotamento de recursos, os usuários não utilizarão ou assinarão nenhum serviço que "transmita" material pela Internet. Isso inclui ouvir música ou estações de rádio pela Internet e receber notícias, informações esportivas e/ou informações do mercado de ações pela Internet.

Além daqueles especificamente atribuídos ou aprovados pelo Gerente Geral, a utilização de ativos de computador de propriedade da Empresa para acessar qualquer conta de e-mail ou serviço por um usuário é expressamente proibida; isso inclui serviços de e-mail como AOL, Hotmail, Gmail e quaisquer outros serviços semelhantes.

Os usuários não revelarão sua senha a ninguém. Excluindo membros da Administração ou um fornecedor de TI designado, no desempenho de suas funções atribuídas, os usuários não utilizarão ou acessarão contas de Internet pertencentes a nenhum outro usuário.

A violação desta política resultará em ação disciplinar até e incluindo a rescisão.

❖ *22.2.2 – Configurações de Segurança*

O Sistema utilizado pela empresa é atualizado anualmente constantemente para conter a linguagem e protocolos de segurança atuais para evitar vazamentos e invasões, assim como limpar qualquer módulos ou funções inutilizadas que possam se tornar um risco.

Todos os softwares deverão estar atualizados em sua versão mais recente, assim que disponível para garantir que não haja vulnerabilidade e acessos indevidos ao computador.

❖ *22.2.3 – Trabalho Home-Office e Remoto*

As mesmas medidas de segurança aplicadas neste sessão para quem trabalha no escritório serão aplicadas para o trabalho home-office e remoto, a empresa irá providenciar os equipamentos como computador com os softwares necessários, telefones de comunicação e provedor de internet onde todo o trabalho desenvolvido para a empresa deverá ser unicamente realizado nos equipamentos providenciados pela empresa.

O uso dos computadores será limitado para acessar o sistema online da empresa e email para o desenvolvimentos das atividades comerciais necessárias.

Os funcionários deverão tomar as mesmas medidas de prevenção aqui listadas nesta sessão como também tomar cuidado extra para não clicar em links suspeitos, promoções ou qualquer site que esteja solicitando informações sensíveis.

❖ *22.2.4 – Controle de Incidentes*

O Gerente de TI é responsável por realizar backups do sistema operacional da empresa e seus emails semanalmente para que em eventual incidente de invasão ou perda de dados o mesmo possa ser restabeelecido dentro de um período máximo de 12 horas para que as operações da empresa não sejam afetados.

Ao se deparar com um problema no sistema operacional ou emails, o Gerente de TI deve imediatamente acessar o servidor e fazer as correções necessárias e caso necessario o desativamento temporário para restauração de backup.

❖ *22.2.4 – Prevenção de Malwares*

O Gerente de TI é responsável em certificar que todos os computadores da empresa estejam equipados com programas antivirus.

Qualquer instalação de programas nos computadores da empresa devem ser aprovados e realizados pelo Gerente de TI para se evitar o risco de instalação de malwares (programas com fins maliciosos para roubar informações).

Os computadores serão configurados para que somente seja possível a instalação de programas através de uma senha master que somente o Gerente de TI terá acesso.

❖ *22.2.5 – Controle de Acesso de usuários*

O sistema operacional da empresa é acessado através de login e senha individual limitado as taredas de cada usuário, limitando assim o acesso a somente informações ao escopo de trabalho e responsabilidade do funcionário.

Areas restritas do sistema não poderão ser acessadas pelo funcionário sem a devida credencial de acesso ou aprovação de acesso por parte do Gerente Geral da empresa.

❖ *22.2.6 – Monitoramento*

O sistema e servidores da empresa devem ser monitorados diariamente pelo Gerente de TI e assisnte visando a segurança e integridade do sistema e emails para o bom funcionamento das operações da empresa,

Os acessos as tarefas realizadas pelos funcionários da empresa são monitorados constantemente através de um registro de logs dentro do sistema para entender as tarefas realizadas e bom funcionamento.

❖ *22.2.7 – Segurança da Internet*

Para evitar a exploração da rede, as principais medidas de segurança incluem: senhas fortes, autenticação multifator, firewalls robustos, sistemas de detecção/prevenção de intrusão (IDS/IPS), atualizações regulares de software, proteção antivírus, monitoramento de rede, criptografia de dados, controles de acesso, treinamento de conscientização de segurança e verificação de vulnerabilidades; garantindo uma abordagem em camadas para proteção contra vários vetores de ataque.

❖ *22.2.8 – Mídias Removíveis(USB/HD Externos,ETC)*

Para evitar riscos de segurança é limitado o uso de midia removiveis (exemplo: USB, HD Externo e outros somente com autorização prévia por escrito do Gerente Geral.

Quando permitido o uso a criptografia é obrigatória de todos os dados em dispositivos removíveis, verificações completas de malware antes de acessar qualquer mídia removível devem ser realizadas, proteção por senha em unidades removíveis devem ser realizadas, medidas de segurança física para evitar perdas ou roubos, treinamento de funcionários sobre o manuseio adequado de mídia removível, restrição de acesso de gravação a mídia removível, implementação de um sistema para rastrear e gerenciar o uso de mídia removível e uso somente de tipos de mídia removível aprovados.

❖ *22.2.9 – Responsabilidade, educação e conscientização do usuário:*

Os funcionários novos receberão um treinamento inicial sobre a segurança cibernética e importância e todos os funcionários serão treinados regularmente sobre a importação de como lidar e agir com responsabilidade afim de evitar riscos de segurança.

As sessões de treinamento serão conduzidas pelo Gerente de TI visando explicar os riscos atuais de acordo com as dificuldades apresentadas atualmente no mundo

e como proteger as informações e evitar riscos a segurança das informações, computadores e sistemas da empresa.