POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ÍNDICE

1 - INTRODUÇÃO

A informação é um dos principais patrimônios do mundo dos negócios, e sendo assim precisa ser preservada de forma a garantir sua integridade e confidencialidade. Para assegurar a metodologia de manter seguras as informações dos bancos de dados da Neweasy e também dos nossos clientes públicos e privados estabelecemos e implementamos a seguinte Política de Segurança da Informação, que dará aos colaboradores diretrizes para a Segurança da Informação, e aos parceiros, fornecedores e clientes a garantia dos nossos esforços de proteção à informação.

Esta Política de Segurança da Informação se aplica aos colaboradores da Neweasy para que sejam capazes de cumprir com os requisitos da **Lei Geral de Proteção de Dados** (Lei 13.709 de 14/08/2018) que tem por objetivo garantir a proteção aos dados pessoais obtidos, inclusive por meios digitais respeitando os direitos fundamentais de liberdade e de privacidade, que possam ser eventualmente violados pela má utilização dessas informações, permitindo maior confiança em relação à coleta e uso de dados, maior segurança jurídica e, em consequência, o fomento ao desenvolvimento econômico e tecnológico da sociedade, à medida que estabelece regras claras sobre a proteção de dados pessoais.

Neste documento apresentamos um conjunto de instruções para normatizar e melhorar nossa visão e atuação com as ferramentas de Tecnologia da Neweasy.

2 - RESPONSABILIDADES

As normas aqui estabelecidas devem ser seguidas por todos os colaboradores, parceiros e prestadores de serviços da Neweasy.

Ao receber esta cópia da ***Política de Segurança da Informação***, o recebedor compromete-se a respeitar todos os tópicos aqui abordados e está ciente de que todos os seus dados, e-mails e navegação na internet/intranet, assim como imagens das nossas câmeras de segurança podem ser monitorados a qualquer tempo.

A equipe de Tecnologia de Informação encontra-se à total disposição para esclarecimentos de dúvidas e auxílio técnico.

Colaboradores - atender esta política de segurança da informação em sua totalidade.

Equipe de TI :

- assegurar a realização de backups de acordo com a periodicidade estabelecida;
- monitorar ferramentas tecnológicas da empresa;
- dar feedback a diretoria de resultados encontrados nas monitorias;
- informar a diretoria sempre que houver violação desta política.

Diretoria - garantir a infraestrutura necessária para a implementação e manutenção desta política e a preservação de dados.

3 - INFORMAÇÕES CONFIDENCIAIS

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponível ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela Neweasy e/ou obtidas pelo colaborador ou terceirizado em decorrência da execução do contrato de prestação de serviços. Aquele que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais podem ser repassadas para terceiros sem consentimento da Neweasy. As informações confidenciais somente poderão ser utilizadas para fins de execução das atividades

contratadas.
São exemplos de informações confidenciais:
Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG, PIS/NIS,CNH,PASSAPORTE,CARTEIRA DE TRABALHO, TITULO DE ELEITOR, CERTIFICADO DE ESCOLARIDADE, CERTIDÃO DE NASCIMENTO, CERTIDÃO DE CASAMENTO, COMPROVANTE DE RESIDENCIA), situação financeira e movimentação bancária; dados de relógios de ponto eletrônico;
Informações sobre produtos e serviços que revelem vantagens competitivas da Neweasy frente ao mercado;
Todo o material estratégico da empresa (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
Quaisquer informações da Neweasy, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;
Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

4 - VIOLAÇÃO DESTA POLÍTICA

As violações de segurança devem ser informadas a Diretoria, ao Gerente Técnico ou ao Departamento de Qualidade da Neweasy. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Exemplos que podem ocasionar sanções:
- uso ilegal de software;
- introdução (intencional ou não) de vírus de informática;
- tentativas de acesso não autorizado a dados e sistemas;
- compartilhamento de informações sensíveis do negócio;
- divulgação de informações de clientes e das operações contratadas;

Os princípios de segurança estabelecidos na presente política possuem total apoio da diretoria da Neweasy e devem ser observados por todos na execução de suas funções. A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita o infrator a penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos. Em caso de dúvidas quantos aos princípios e responsabilidades descritas nesta norma, deve-se entrar em contato com a Diretoria Técnica, com o Gerente Técnico ou com o Departamento da Qualidade da Neweasy.
O não comprimento desta política acarretará em sanções administrativas em primeira instância, podendo acarretar no desligamento do funcionário e ações judiciais de acordo com a gravidade da ocorrência.

5 - EQUIPAMENTOS E SOFTWARES

5.1. Equipamentos: Apenas os *equipamentos* disponibilizados e equipamentos autorizados pela Neweasy podem ser instalados e conectados à rede da empresa. Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

5.2. Softwares: Apenas *softwares* devidamente licenciados podem ser instalados nas máquinas da Neweasy. O setor operacional é responsável por manter as licenças válidas.
Os softwares desenvolvidos pelos Programadores contratados pela empresa são de propriedade intelectual da Neweasy. Os desenvolvedores de softwares devem manter disponível para a Diretoria toda a documentação lógica dos softwares desenvolvidos, atendendo todas as boas práticas de engenharia de software.

6 - ACESSO A SISTEMAS E RECURSOS DE REDE

O usuário é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes. O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função. Periodicamente, os acessos concedidos podem ser revistos pela equipe de Tecnologia da Informação.

6.1 - Autenticação

O usuário é responsável por todos os atos executados com seu identificador (login), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia. Os usuários devem:
- *Manter a confidencialidade,* ***Senhas*** *são* ***pessoais*** *e* ***intransferíveis*** *. Jamais anote, compartilhe ou informe em qualquer local não confiável;*
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Selecionar senhas de qualidade, que sejam de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

Nota: Senhas como nome do usuário, combinações simples (abc123), substantivos (casa, meia, cadeira, brasil), datas (11092001) e outros são extremamente inseguros. Então a Neweasy orienta que sejam criadas senhas de forma coerente, observando nossa política de senhas.

6.2 - Política de Senhas

Uma senha segura deverá conter no mínimo 8 (oito) caracteres, quando o sistema permitir, quando não seguir os avisos informados pelo sistema. Para criar uma senha com boa segurança use sempre letras maiúsculas e minúsculas, números e símbolos (@#$%*).

Por Exemplo:
N3w3@sy1
Lkd#$%&
Ghdae#@*(

7 - POLÍTICA DE EMAIL

Não se deve tentar abrir anexos de E-mails não que fazem parte da sua lista de e-mails, desconfie de qualquer e-mail que tenha anexo com títulos em negrito ou mesmo com respostas em urgente.
Em caso de dúvida use de cautela e verifique com o responsavel técnico como proceder.

Não se deve confiar nos e-mails e anexos com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: 'ILOVEYOU', 'Branca de neve', 'Você foi traído', etc.

Não são permitidos e-mails do tipo corrente. Exemplos: 'aviso de vírus', 'avisos da Microsoft/Symantec', 'criança desaparecida', 'criança doente', 'pague menos em alguma coisa', 'não pague alguma coisa', etc.

Não é permitido utilizar o e-mail da empresa para assuntos pessoais.

Deve-se evitar anexos muito grandes, limitado ao que esta configurado no provedor de e-mail.

- Utilize sempre sua assinatura criptográfica no ***padrão da empresa*** para troca interna e externa de e-mails, conforme exemplo abaixo:

8 - POLÍTICAS DE ACESSO A 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 similares estará bloqueado e monitorado.

NOTA: O uso da internet é monitorado e poderá ser auditado.

9 - USO DA ESTAÇÃO DE TRABALHO
Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede, e cada indivíduo possui sua própria estação de trabalho. Isso significa que tudo que venha a ser executado na estação de trabalho é de responsabilidade do usuário logado. Por isso, ao sair da estação de trabalho, o usuário deve assegurar que efetuou logoff ou travou o console.

Não instale nenhum tipo de software / hardware sem autorização da equipe técnica ou de segurança.

Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria.

Mantenha na sua estação somente o que for supérfluo ou pessoal. Todos os dados relativos à empresa devem ser mantidos no servidor, onde existe um sistema de backup diário e confiável. Caso não saiba como fazer isso, entre em contato com a equipe técnica.

10 - DISPOSITIVOS MÓVEIS
A Neweasy deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.
Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Diretoria, como: notebooks, smartphones e pendrives.
Esta norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores e terceirizados que utilizem tais equipamentos.
A Neweasy, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de

inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança. O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Neweasy, mesmo depois de terminado o vínculo contratual mantido com a instituição.
Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.
O suporte técnico aos dispositivos móveis de propriedade da Neweasy e aos seus usuários se dá pela equipe de Tecnologia da Informação da empresa.
Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da equipe de Tecnologia da Informação.
O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela equipe de Tecnologia da Informação da Neweasy.
É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Neweasy, notificar imediatamente seu gestor direto e a equipe de Tecnologia da Informação. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).
O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracteriza a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a Neweasy e/ou a terceiros.
O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Neweasy deverá submeter previamente tais equipamentos a equipe de Tecnologia da Informação.

NOTA: A Neweasy não se responsabilizará pelos conteúdo ocupado no dispositivo. Assim como não será responsável pelo backup do conteúdo de conversas contidas em aplicativos Instant Messengers.
Cabe ao proprietário do dispositivo, efetuar o backup de seu conteúdo.

11 - DATACENTER
O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.
Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.
Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.
O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do Gerente Técnico.
O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.
O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a Diretoria ou ao Gerente Técnico.
Deverão existir três cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do Gerente Técnico, as outras, de posse dos Diretores.
O Datacenter deverá ser mantido limpo e organizado.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável. A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com a autorização formal do Gerente Técnico ou dos Diretores.
No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte.

12 - POLÍTICA SOCIAL
Como seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando discorremos sobre segurança, isso é uma desvantagem. Por isso observe os seguintes tópicos:

Não fale sobre a política de segurança da empresa com terceiros ou em locais públicos.

Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha.

Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa.

Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado.

Nunca execute procedimentos técnicos cujas instruções tenham chegado por e-mail.

Relate a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

13 - VÍRUS E CÓDIGOS MALICIOSOS
Mantenha seu antivírus atualizado. Provavelmente nossa equipe técnica irá se encarregar disso, mas caso não tenha sido feito ou você perceba que a atualização não está funcional, entre em contato com a mesma para que a situação possa ser corrigida.

Não traga Pendrives, CD's ou HD's de fora da empresa. Caso isso seja extremamente necessário, encaminhe o mesmo para a equipe técnica, onde passará por uma verificação antes de ser liberado para uso.

Comunique atitudes suspeitas em seu sistema a equipe técnica, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.
Suspeite de softwares que "você clica e não acontece nada".

14 - BACKUP DAS INFORMAÇÕES
Todos os backups devem ser automatizados por sistemas de agendamento automáticos para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.
Para proteção dos dados armazenados em nossos servidores, a Neweasy implantará a seguinte rotina de backup:

14.1 - Backup Diário

Diariamente, por volta das 00:00, serão executados scripts de backup incremental em todos os servidores de Banco de Dados. O backup diferencial é administrado pela ferramente Google Drive, aonde o mesmo salva as informações em tempo real dos arquivos modificados e fechados pelo usuários.

Os colaboradores responsáveis poderão delegar a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar.

15. MESA LIMPA

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não. Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.
Conversas em Locais Públicos e registro de informações
Não discutir ou comentar assuntos confidenciais em locais públicos.

16 - CONFIABILIDADE DOS NEGÓCIOS

A Neweasy conta com a sua colaboração para que a empresa seja reconhecida por seus altos padrões de segurança em tecnologia da informação, passando para os nossos clientes confiabilidade.
Entre em contato conosco sempre que julgar necessário.

17 - MEMBROS DA EQUIPE DE TECNOLOGIA DA INFORMAÇÃO

Nome	**E-mail**	**Celular**
Henrique Carvalho	henrique@neweasy.com.br	22 99899-3050
Natanael Ferreira	projetos@neweasy.com.br	22 99911-9797

18 - DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Neweasy. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela empresa.