Política de Segurança da Informação

1. Objetivo e Aplicação

1.1. Objetivo da Política

Esta Política de Segurança da Informação ("Política") visa orientar as ações, procedimentos e diretrizes para o uso dos ativos de Informação da Enauta Participações S.A. e da Enauta Energia S.A. (conjuntamente, "Enauta"), ou a elas confiados, a fim de garantir a confidencialidade, integridade, disponibilidade e privacidade (quando aplicável) das Informações, sendo aplicável a todos os colaboradores da Enauta.

1.2. Segurança da Informação Como Cultural Organizacional

Na Enauta entendemos que segurança é parte principal da cultura e DNA da empresa. Entendemos e acreditamos em uma abordagem de "Segurança por *Design*", onde toda a construção do negócio é feita em uma base sólida em segurança.

Qualquer sistema, processo, procedimento e controle são concebidos em torno da segurança.

A cultura da segurança por 'design' deve ser adotada internamente por todos os colaboradores e parceiros. Para fornecedores, esta previsão deve estar explícita em cláusulas contratuais, assim como suas cadeias de relacionamento em primeiro nível.

Todos esses esforços convergem para a proteção dos ativos de Informação do ecossistema "Enauta", principalmente seus clientes colaboradores, parceiros de negócios e acionistas.

1.3. O Que é Segurança da Informação?

Segurança da Informação ("SI" ou "Segurança da Informação") é a proteção da Informação contra vários tipos de ameaças, para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades para a Enauta ou seus clientes.

A Segurança da Informação é obtida a partir da implementação de um conjunto de controles, incluindo tecnologia, políticas, processos, procedimentos e a própria estrutura organizacional da empresa.

Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente, sempre que necessários, e melhorados continuamente para garantir que os objetivos e a segurança da Enauta sejam atendidos.

Internamente, considera-se como informação toda a base de conhecimento, conteúdo, dado, conceito, envio ou recebimento de mensagem, processo ou fato existente, em meio físico ou eletrônico, que compõe documentos e Informações de propriedade, interesse ou posse da Enauta e inclui, mas não se limita a, qualquer dado, material, procedimento, processo, especificações, inovações e aperfeiçoamento técnicos e comerciais que agreguem valor para o negócio da empresa, assim como todas as informações confidenciais dos nossos clientes sob nossa custódia ("Informação(ões)").

1.4. APLICAÇÃO

A Segurança da Informação é crítica para o negócio da Enauta e, por isso, carregamos a "Segurança" como mais que um requisito para o negócio, *Segurança é o principal valor da nossa cultura.*

Sendo assim, temos como principal objetivo deste documento estabelecer as diretrizes necessárias para orientar a todos os membros de nossa equipe os cuidados a serem observados para a manutenção de nossas Informações em um padrão de segurança superior.

2. NORMAS DE REFERÊNCIAS

2.1. BASES E REFERÊNCIAS PARA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Este documento está fundamentado nos Objetivos de Controle elencados pela norma ABNT NBR ISO/IEC 27002, assim como as publicações NIST e seu Framework de Segurança da Informação.

Confidencialidade: não permitindo disponibilização ou exposição da Informação a indivíduos, entidades ou processos não autorizados expressamente, seja por contratos ou outros instrumentos formais.

Integridade: salvaguardando exatidão e completeza das Informações, tal como foram criadas ou recebidas utilizando tecnologias, controles e processos que garantam esse requerimento pelo próprio design dos produtos e sistemas do Enauta.

Disponibilidade: os sistemas e Informações pertencentes ao ecossistema tecnológico do Enauta deverão estar disponíveis para seus clientes, associados e colaboradores, atendendo também a confidencialidade das Informações e integridade de seu conteúdo, formando, assim, uma tríade de Segurança de qualidade superior.

Privacidade e Proteção de Dados Pessoais: os dados pessoais contidos nas Informações devem ser protegidos com a adoção de medidas técnicas e organizacionais de Segurança da Informação, nos termos impostos pela Lei nº 13.709/2018, conhecida por LGPD ou Lei Geral de Proteção de Dados e que estará disciplinada em conjunto com o Procedimento de Tratamento de Dados Pessoais e o Código de Conduta Ética.

3. ABRANGÊNCIA

3.1. OBJETIVOS E CONTROLES

Para a presente Política, deverão ser seguidos por todos os colaboradores da Enauta, **independentemente de sua relação contratual e nível hierárquico** e são aplicáveis a toda Informação da empresa, seus clientes e usuários, em qualquer fase de seu ciclo de vida e meio ou suporte que os mesmos se encontrem, tais como, mas não se limitando a: mídias físicas, mídias eletrônicas, transmissão de dados ou mesmo pela transmissão verbal.

Esta Política ficará disponível na sua íntegra e sempre em sua versão aprovada mais recente, em nossas ferramentas de comunicação, quais sejam: Gestor, intranet e site institucional.

4. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

4.1. ORGANIZAÇÃO E ESTRUTURA ORGANIZACIONAL APLICADAS À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Os **Diretores**, em nível estratégico, apoiam ativamente a cultura de Segurança da Informação como valor estratégico na empresa, por meio de um claro direcionamento, demonstrando o seu comprometimento, tal como demonstrado na aprovação formal desta Política de Segurança da Informação.

São atribuições específicas do **Diretor-Presidente**:

- Definir a estratégia de Segurança da Informação para a Enauta, alinhando a mesma às demais estratégias do negócio;
- Deliberar sobre a criação, organização, estrutura e regulamentação de um Grupo de trabalho de Segurança da Informação e Privacidade de Dados
- Convocar e coordenar, a seu critério, reuniões periódicas e emergenciais deste Comitê;
- Aprovar os documentos estratégicos.

O **Grupo de Segurança da Informação** terá uma atividade cooperativa, colaborativa e contínua, e será composto pelos membros dos departamentos de TI, Jurídico e Compliance, além do DPO.

São atribuições específicas do **Grupo de Segurança:**

- Elaboração e revisões da Política de Segurança da Informação da Enauta, o qual servirá como guia para as ações de educação e difusão cultural do tema de Segurança da Informação e os controles técnicos aplicáveis;
- Revisão das ações educacionais já existentes na Enauta, como treinamento específico sobre SI para novos colaboradores além de iniciativas recorrentes de atualização para os demais

colaboradores, objetivando uma reciclagem total em até 18 meses para todos os colaboradores e associados da Enauta.

- Revisão dos procedimentos para continuidade dos negócios da Enauta (Plano de Continuidade de Negócios), bem como a produção e implantação de novos procedimentos que garantam a operação contínua dos negócios e da Enauta frente aos riscos mapeados pelo comitê gestor de riscos;
- Participação ativa no Comitê de Gestão de Crises, incluindo a atualização de procedimentos em conformidade com esta Política e com as estratégias da marca;
- Participação ativa nas revisões dos procedimentos de Gerenciamento de Mudanças ("Change Management") no ambiente computacional da Enauta;
- Fomento à cultura de Segurança da Informação dentro da Enauta e em toda a cadeia de relacionamentos incluindo, Clientes, Fornecedores, Parceiros de Negócios, Colaboradores e Associados;

Todos os sócios, empregados, colaboradores, associados, incluindo terceiros ou quaisquer prestadores de serviços recorrentes da Enauta, independentemente da relação contratual estabelecida e do nível hierárquico, são responsáveis por:

- Conhecer e cumprir rigorosamente a Política de Segurança da Informação da Enauta, bem como toda a documentação correlata;
- Pela ótica da responsabilidade pela segurança, todos na Enauta são colaboradores e devem se atentar e reportar ao se deparar com práticas em não conformidade com a Política de Segurança, ajudando, inclusive, na reeducação dos hábitos em não conformidade;
- Reportar ao Comitê de Segurança da Informação, ou ao canal disponibilizado pela mesma, a suspeita ou confirmação de descumprimentos de toda a documentação de SI e seus Objetivos de Controle, bem como de tentativas de burla de recursos e ferramentas de SI e quaisquer incidentes de SI;
    - As seguintes práticas podem ser entendidas como incidentes de SI: (i) acesso não autorizado a recursos de TI, sistemas e banco de dados da Enauta ou de terceiros; (ii) vírus; (iii) ataques de navegação de serviços (DoS ou DDoS); (iv) violação a esta Política ou procedimentos de SI correlatos; (v) acesso não autorizado ou vazamento de dados, inclusive de dados pessoais que estejam sob custódia da Enauta; (vi) uso impróprio de Informações; (vii) pirataria; (viii) falha do equipamento da Enauta.

5. CLASSIFICAÇÕES

5.1. CLASSIFICAÇÃO DA INFORMAÇÃO E MINI GLOSSÁRIO

A Informação é tida como um ativo e possui valor diferente dependendo do seu conteúdo. Os controles de proteção desses ativos podem aumentar de acordo com seu valor. A classificação das Informações também pode definir quais controles de proteção precisam ser implementados.

Podemos entender a classificação da Informação também como uma escala de proteção a ser aplicada na mesma.

Para a Enauta, são cinco os níveis de classificação da Informação em ordem crescente de importância e sigilo:

PÚBLICAS: são todas as Informações que já sejam de conhecimento público e estejam disponibilizadas para Clientes, Colaboradores e Público em Geral através da Internet, ou veiculadas em documentos publicados em jornais, revistas, folders, redes sociais, panfletos, avisos ou palestras autorizadas. Somente as áreas de Relação com Investidores, Relações Externas e Sustentablidade poderão publicar Informações sobre a empresa ou "em nome da Enauta", bem como definir e orientar porta-vozes do negócio.

INTERNAS: são Informações que estão disponíveis aos colaboradores por meio das ferramentas aprovadas, com armazenamento interno, em servidores da Enauta ou terceiros autorizados (na nuvem, por exemplo). Qualquer Informação classificada como "INTERNA" não poderá ser encaminhada, divulgada ou publicada em quaisquer meios para terceiros não autorizados, devendo a sua disponibilização ser restrita ao ambiente de trabalho da Enauta e uso limitado aos Colaboradores ou terceiros (mediante assinatura de termo de "não divulgação" - NDA), que realmente necessitem ter acesso a tais Informações.

RESTRITAS: os documentos classificados como "INFORMAÇÃO RESTRITA" somente poderão ser acessados pela área, departamento, setor ou função dentro da Enauta que classificou a Informação. Normalmente são Informações de uma determinada área que não deve ser acessada por outros setores da empresa, por exemplo, os documentos do setor de RH ou departamento financeiro da empresa.

CONFIDENCIAL: todas as Informações classificadas como confidenciais deverão ser mantidas em arquivos físicos ou eletrônicos com níveis de segurança compatíveis com a relevância da Informação, tais como cofres, armários com chaves, diretórios criptografados ou envio dos arquivos somente após a inclusão de mecanismos de segurança (senha ou criptografia). A transmissão de arquivos confidenciais só deverá ser feita utilizando meios de transmissão seguras, para as partes previamente autorizadas, com contrato de sigilo claro e dentro da validade, sejam as partes: funcionários, colaboradores, associados, fornecedores ou qualquer tipo de parceiro de negócios que precisam: criar, armazenar ou processar qualquer tipo de Informação CONFIDENCIAL.

ARMAZENAMENTO E TRANSMISSÃO DE INFORMAÇÕES CONFIDENCIAIS:

Atendendo aos requisitos contratuais de sigilo, os meios de armazenamento previamente aprovados são: discos criptografados, transmissão por rede ou internet utilizando SSL (com certificado de origem e destino da transmissão pertencentes às

partes acordadas em contrato), SSH ou SFTP (FTP via SSH). Para transmissão de Informações confidenciais por e-mail em servidores e domínios diferentes, é necessário adicionar criptografia adicional em nível de arquivo (senha no arquivo utilizando criptografia forte de no mínimo AES 1024 bits ou equivalente). A proteção por senha deve ser aplicada INCLUSIVE para proteção de certificados privados de uso geral (por exemplo, ao se gerar pares de chaves SSH, é necessário aplicar senha FORTE nas chaves privadas).

Deverão ser classificadas como CONFIDENCIAIS as Informações que por sua origem, natureza ou importância não devam ser compartilhadas ou colocadas à disposição de pessoas não autorizadas. Consideram-se Informações confidenciais todas as que assim forem classificadas, bem como – indistintamente – dados recebidos ou compilados de/sobre clientes, senhas, Informações financeiras ou de salários, código fonte, Informações sensíveis de usuários entre outras.

SECRETAS: as Informações classificadas como SECRETAS possuem o mais alto nível de sensibilidade e criticidade para o negócio. Chaves de criptografia (certificados SSL ou chaves SSH) e credenciais de acesso em geral são exemplos de Informações SECRETAS. Outras Informações estratégicas com alto nível de confidencialidade também podem ser classificadas como SECRETAS a critério do proprietário da Informação.

Informações em que seu possível vazamento implica em impacto financeiro direto ao negócio ou ponha em risco a continuidade dos negócios é um indício para que ela receba a classificação máxima de proteção: SECRETA.

As Informações SECRETAS normalmente possuem os seguintes controles e proteções:

- *São armazenadas em volumes criptográficos acrescidos de criptografia de arquivo: criptografia multinível com chaves e algoritmos distintos.*
- As Informações SECRETAS não podem ser copiadas, fotografadas, filmadas (incluindo sistemas de CFTV) ou testemunhadas, pessoalmente ou por meio de telepresença de qualquer forma.
- Algumas Informações SECRETAS podem simplesmente não ser armazenadas (*brain storage only*), processadas ou transmitidas no ambiente computacional do Enauta sempre que isso for possível.
- O armazenamento das Informações SECRETAS só pode ocorrer em regime de exceção em sistemas offline ou sistemas online aprovados nesta Política:

    a. **Senhas e Credenciais** corporativas de acesso: só poderão ser armazenadas na sua memória ou por meio de software de gestão de senhas (PREFERENCIALMENTE. Ex.: LastPass).

b. Quaisquer senhas armazenadas nos sistemas internos aprovados, para colaboradores e clientes só deverão ser armazenadas utilizando conversão em HASH (SHA256 ou superior) adicionada de técnicas de SALT, técnicas conhecidas como boas práticas de segurança mínima para armazenamento de senhas. Deste modo, TODAS AS SENHAS dentro dos sistemas de Informações da Enauta, para acesso interno ou externo (pelos clientes por exemplo), somente são conhecidas pelo seu proprietário. Nem o Diretor Presidente da Enauta possui acesso à senha de qualquer usuário dos sistemas internos a não ser o proprietário da conta de acesso (cliente ou colaborador).
c. Tamanho de senha mínimo recomendável: mínimo de 9 caracteres e obrigação do uso de 4 opções (maiúsculo, minúsculo, character especial e numeral). Também serão aplicadas restrições a palavras comuns como: Enauta, Petroleo, Gás e etc.

HASH: função criptográfica de via única em que uma sequência de dados gera uma saída única de tamanho fixo que não pode ser revertida. Ou seja, conhecendo o HASH não é possível conhecer a Informação que o gerou.

SALT: trata-se de uma técnica para aumentar a segurança do HASH e evitar ataques do tipo dicionário, onde de posse de um banco de dados de palavras e seus respectivos HASH, se possa chegar a sequência, neste caso a senha em formato aberto.

				Secreta
			Confidencial	
		Restrita		
	Interna			
Pública				

A classificação dos documentos deverá ocorrer em campo visível, preferencialmente na primeira página e próximo ao cabeçalho do Documento.

Quando um Documento contiver mais de um tipo de Informação com classificação original distintas, por exemplo, dois documentos unidos em um único arquivo, a classificação mais restritiva passa a valer para todo o documento.

Qualquer Informação que não tenha sua classificação especificadade forma clara no documento será automaticamente considerada como Informação “RESTRITA”.

6. Deveres e Responsabilidades

6.1. Atribuição Inicial da Classificação à Informação

Caberá ao colaborador AUTOR da Informação definir os acessos, níveis de permissão e formas de proteção quando se tratar de uma Informação RESTRITA, CONFIDENCIAL ou SECRETA.

Será considerado como AUTOR da Informação o colaborador que primeiro produzir ou manipular a Informação dentro do ambiente da Enauta.

Todo colaborador será responsável pela sua classificação e armazenamento, seguindo as recomendações contidas neste documento.

Caberá à área de Segurança da Informação de TI, prover o suporte técnico aos autores das Informações geradas e realizar os devidos treinamentos sobre proteção e armazenamento seguro de dados.

A área de Tecnologia da Informação é a provedora dos recursos e meios de armazenamentos seguro dessas Informações, assim como as ferramentas de controle de acesso, proteção e criptografia.

Caberá ao colaborador armazenar os arquivos digitais da empresa obrigatoriamente no servidor de arquivos por meio dos compartilhamentos carregados em sua estação de trabalho. A área de Tecnologia da Informação não realiza nenhum tipo de backup de dados armazenados de forma local nos equipamentos e não se responsabiliza por arquivos salvos nos mesmos.

6.2. Publicação de Informações Abertas

Somente os gestores da Enauta, com assessoria devida da área de comunicação, poderão classificar Informações para divulgar externamente ou as definir como Informação Pública.

6.3. Descarte de Informação Classificada

As Informações classificadas como RESTRITA, CONFIDENCIAL ou SECRETA devem sofrer tratamento especial no seu descarte.

O descarte de Informações, armazenadas em meio físico ou eletrônico, deverá ser realizado segundo o procedimento de descarte aplicável para garantir que a Informação descartada não possa ser recuperada de qualquer forma.

Além dos demais procedimentos aplicáveis, (i) todas as Informações impressas deverão ser trituradas antes de seu descarte; aparelhos eletrônicos devem ser "resetados" antes de seu descarte; e (ii) Informações eletrônicas deverão ser deletadas mediante o uso de ferramentas apropriadas ao descarte de dados (*NIST 800-88 Data Sanitization)*, a ser disponibilizada pela área de TI/SI da Enauta.

6.4. EXTRAVIO DE INFORMAÇÃO

Qualquer evento de perda, extravio ou roubo de Informações, devem ser reportados IMEDIATAMENTE ao Comitê de Segurança da Informação, por meio do email segurancasi@enauta.com.br.

6.5. DO USO DOS ATIVOS DE TI (FERRAMENTAS CORPORATIVAS)

A Enauta poderá fornecer ao colaborador conta de correio eletrônico, acesso à internet e outras ferramentas de comunicação e produtividade para a dinamização do trabalho ou utensílios como aparelho e linha cellular, gavetas, armários e quaisquer dispositivo, físico ou lógico, para a execução do trabalho.

O uso destas ferramentas estará sujeito a esta Política e restrições de acesso, de acordo com o nível de acesso outorgado ao usuário e deliberações do Comitê de Segurança da Informação.

Como política de nível de acesso à Informação, utilizamos a premissa de "menor privilégio possível". O colaborador somente terá acesso aos aplicativos e Informações que forem estritamente necessários para a realização do seu trabalho.

É expressamente proibido o uso de qualquer recurso corporativo, computadores, redes, acessos bem como quaisquer meios de comunicação corporativas para uso pessoal e/ou prática de qualquer ato ilícito, sob pena de responsabilização civil ou até criminal.

O colaborador é responsável pelos ativos de TI da Enauta, bem como pelas Informações que inserir em tais ativos.

6.6. ACESSO E USO DA INTERNET

A Enauta poderá permitir acesso à Internet e a navegação em sites de conteúdo, sempre de acordo com a sua política de Segurança da Informação e bloqueios de sites classificados como inseguros ou não confiáveis.

É explicitamente proibido a transferência de arquivos por meio de quaisquer protocolos, aplicativo ou ferramenta que não forem previamente e explicitamente aprovados pela área de Segurança da Informação da Enauta.

Essa aprovação é uma análise de segurança da ferramenta e do fornecedor do produto, a fim de garantirmos que somente ferramentas e fabricantes que possuam alta maturidade em Segurança da Informação, proteção de dados e políticas claras de privacidade, sejam incorporados à lista de ferramentas e fornecedores aprovados.

Isso evita a herança de vulnerabilidades por meio de ferramentas não seguras e não testadas, assim como parcerias com fornecedores que possam não seguir as boas práticas de Segurança da Informação.

Da mesma forma, não será permitido o *download* de materiais protegidos por direitos autorais ou a instalação de softwares não homologados pela área de Segurança da Informação. O colaborador deve consultar o departamento de TI antes de fazer o download de qualquer software de terceiro.

6.7. E-MAIL / CORREIO ELETRÔNICO

O correio eletrônico da Enauta, assim como todas as plataformas de comunicação utilizadas na empresa, são ferramentas de trabalho, não devendo ser utilizado para outros fins.

As Informações contidas nas mensagens eletrônicas são de propriedade da Enauta podendo ser monitoradas a qualquer tempo sem aviso ou notificação prévia para fins de auditoria de conformidade às normas internas, regulamentações ou boas práticas aplicadas ao negócio da Enauta. (Veja o item MONITORAÇÃO nesta mesma Política)

É expressamente proibido o envio de Informações classificadas como “INTERNAS” e “CONFIDENCIAIS” para endereços de e-mail para endereços de outros domínios além da Enauta.com.br, exceto para terceiros (clientes ou fornecedores) diretamente envolvidos no respective assunto da mensagem.

As Informações classificadas, como “SECRETAS” não devem ser armazenadas ou transmitidas por e-mail simples. Para isso, é obrigatório o uso de criptografia forte adicional para proteção do conteúdo da mensagem e seus anexos, através de solicitação à área de Segurança de Informação e autorização do superior imediato.

Quando um coladorador da Enauta for desligado, deverão ser observados os seguintes procedimentos em relação ao seu e-mail corporativo:

- O colaborador, independente de seu cargo, deverá ser informado de que seu e-mail corporativo foi suspenso e que o colaborador poderá, desde que acompanhado por um outro colaborador da Enauta designado para essa tarefa, retirar eventual e-mail pessoal e informações pessoais constantes em sua caixa de e-mails corporativa e/ou arquivos digitais e físicos;

- O e-mail corporativo do colaborador desligado deve emitir mensagem resposta ao receber e-mails informando que o e-mail está suspenso e que o remetente poderá entrar em contato com a Enauta por meio de outro canal de comunicação (por exemplo, e-mail de eventual gestor do colaborador desligado);
- O e-mail corporativo deve ficar ativo somente por um prazo razoável de até 3 meses e após esse período deve ser excluído juntamente com todas as Informações e dados pessoais.

6.8. SENHAS DE ACESSO

A senha de acesso aos recursos computacionais da Enauta é de inteira responsabilidade do colaborador, que não deverá, em hipótese alguma, compartilhar ou emprestar a outros colaboradores e terceiros.

Os usuários deverão utilizar senhas "fortes", misturando letras e números, em todos os sistemas corporativos e o tamanho mínimo recomendado para as senhas é de 9 (nove) caracteres.

Informações classificadas como SECRETAS deverão obrigatoriamente utilizar uma sequência longa de pelo menos 16 caracteres, ou optar pela utilização de uma chave criptográfica de pelo menos 1024 bits (utilizando-se sempre uma senha adicional para a proteção da chave criptográfica).

Toda ação feita, dentro ou fora do ambiente computacional da Enauta, será de responsabilidade do colaborador associado às credenciais de acesso associadas às ações.

6.9. CONTAS INATIVAS

Toda e qualquer credencial de acesso que não tiver atividade em até 30 dias serão bloqueadas em TODOS os sistemas corporativos.

6.10. AUTENTICAÇÃO DE MULTI FATOR (DOIS FATORES)

É obrigatório o uso de autenticação multi-fator (2FA ou MFA; Two factor Authentication ou Multi-Factor Authentication) para TODOS os serviços onde a opção estiver disponível.

6.11. ACESSO REMOTO

Colaboradores previamente cadastrados, mediante aprovação explícita dos seus gestores diretos, poderão obter acesso remoto ao ambiente computacional da Enauta para trabalho for a de seu ambiente normal. Para isso, é necessário a abertura de chamado com aprovação da gestão.

Esse processo deve utilizar apenas equipamentos corporativos fornecidos pela Enauta com a aplicação dos controles de segurança vigentes. A conexão será estabelecida por meio de VPN privada corporativa.

6.12. MESA LIMPA

Todos os colaboradores deverão obedecer às regras de limpeza e organização do ambiente de trabalho a fim de não expor desnecessariamente Informações classificadas.

Os documentos impressos e anotações que precisem estar em um papel (impresso ou anotações) devem permanecer nas mesas em caráter temporário devendo ser recolhidos em compartimentos fechados disponíveis em seu departamento ou qualquer dependência da empresa que forneça segurança e proteção a esses materiais.

Toda Informação que permanecer nas mesas poderá e deverá ser destruída pelo colaborador responsável ou por qualquer outro colaborador que assim o quiser fazê-lo exercitando as boas práticas de proteção de Informações da Enauta.

Os documentos órfãos notoriamente importantes (que possuem assinaturas por exemplo) deverão ser depositados em um armário especial do tipo boca de lobo para que possam ser revisados posteriormente antes de sua destruição - cofre de documentos órfãos localizados ao lado das impressoras.

Esta regra vale para o ambiente de trabalho, incluindo a estação de trabalho, mesa, gavetas, arquivos e lixo.

6.13. BLOQUEIO DE DISPOSITIVO POR INATIVIDADE

Todo dispositivo corporativo de acesso aos sistemas corporativos deve sofrer bloqueio automático depois de 10 minutos de inatividade (computadores, smartphones, tablets ou qualquer outro dispositivo, móvel ou não).

6.14. CAPTURA DE TRÁFEGO NA REDE

É expressamente proibido a captura de tráfego de rede dentro da rede corporativa da Enauta salvo eventos devidamente autorizados pelo Comitê de Segurança ou pelo gestor de segurança para fins exclusivos de diagnóstico, auditoria e monitoração previamente autorizados.

6.15. DISPOSITIVOS PESSOAIS

O uso de dispositivos pessoais fica restrito a rede de **convidados/guest** da Enauta.

Não é permitido a conexão de dispositivos não corporativos as redes internas, cabeadas ou sem fio.

Aos colaboradores que precisem fazer uso de dispositivos móveis para o desempenho de funções e tarefas específicas, o farão utilizando equipamentos fornecidos pela empresa, com os devidos controles e proteções técnicas aplicadas.

6.16. REDES SOCIAIS

É expressamente proibido que qualquer colaborador emita qualquer comunicado, opinião ou comentário EM NOME da Enauta sem a expressa aprovação e alinhamento com as áreas de marketing e comunicação.

As interações de resposta, réplica aos comentários feitos por terceiros sobre a empresa e afins, só podem ser feitas pelas áreas específicas de comunicação e gestão de mídias sociais, mesmo sendo postadas em redes pessoais.

A publicação de fotos em área internas também deve ser evitada, para evitar que Informações restritas contidas nas áreas internas da empresa sejam publicadas inadvertidamente, a não ser que seja previamente autorizada pela área de comunicação

6.17. SOFTWARE, APPS E PLUGINS

Não é permitido a instalação de softwares não aprovados pela área de TI e Segurança de Informação em quaisquer dispositivos que acessam os sistemas de Informação da Enauta que inclui: computadores, notebooks e dispositivos portáteis como tablets e celulares. Inclusive software, aplicativos, plugins pagos ou gratuitos.

A área de TI e SI devem possuir um portfólio de ferramentas e aplicativos para atender as demandas do negócio incluindo ferramentas de produtividade e afins.

A maioria dessas ferramentas já são previamente instaladas em todos os dispositivos corporativos.

6.18. POSTURA GERAL DE PRIVACIDADE

Todos os acessos aos sistemas internos devem ter como justificativa um propósito real de negócio.

É expressamente proibido o acesso a quaisquer Informações de clientes, colaboradores ou qualquer registro nos sistemas de Informação da Enauta sem um propósito claro de negócio, e ligado diretamente ao exercício das funções atribuídas na relação de trabalho entre o colaborador e a empresa.

É expressamente proibido o acesso a dados de clientes por mera curiosidade, por exemplo:

- Acessar contas de celebridades, pessoas públicas, parentes, amigos ou qualquer outro cliente sem que haja um propósito de negócio e principalmente, um chamado relacionado ao caso.
- Caso precise resolver algum problema na sua própria conta, como alterar uma Informação de cadastro, abra um chamado e peça que um colega faça a alteração para você.

6.19. MONITORAÇÃO

A Enauta se reserva ao direito de monitorar todas as atividades feitas pelos seus colaboradores em seus sistemas de Informação para garantir o cumprimento desta e outras políticas da empresa.

Os ambientes internos da Enauta também podem sofrer gravação audiovisual com o propósito principal de gerenciar a segurança do perímetro interno da empresa contra incidentes de segurança de qualquer natureza.

6.20. MOFIFICAÇÃO / ROOT / JAILBREAKING

Com o propósito de proteger os dados da Enauta e seus clientes, não é permitido acessar qualquer ferramenta corporativa utilizando dispositivos que sofreram alterações nos sistemas nativos de segurança.

Exemplos práticos:

- Acesso utilizando celular ou tablet Android com alterações e desbloqueios, conhecidos também como "Root de Android";
- Acesso utilizando um iPhone ou iPad com "Jailbreak".

Devido a criticidade e o entendimento de que essas modificações afetam seriamente a segurança desses dispositivos, acessos feitos a partir de dispositivos pessoais (qualquer celular ou tablet pessoal) com essas modificações é **expressamente proibido**.

6.21. ACESSO AO ESCRITÓRIO E ESCOLTA DE VISITANTES

O acesso aos nossos escritórios NÃO pode ser feito por pessoas DESACOMPANHADAS. O anfitrião do visitante deverá acompanhá-lo, DESDE a chegada na recepção da Enauta, até a entrada no escritório. Quem não possui biometria cadastrada ou crachá de acesso, sempre terá que ser acompanhado pelo seu anfitrião ou por um colaborador da Enauta.

Para colaboradores ou consultores externos que trabalhem mais de dois dias por semana no escritório, iremos cadastrar sua biometria ou crachá e liberar o acesso sem escolta.

A porta principal DEVE PERMANECER SEMPRE FECHADA, mesmo para saídas rápidas do escritório (colocar detritos e lixos no compartimento do andar, por exemplo). Antes de abrir a porta, sempre OBSERVE com cuidado QUEM está no hall dos elevadores, na parte externa do escritório. Se houver presença de estranhos NÃO abram a porta, retornem para a recepção e aguarde alguns minutos antes de retornar ao andar. Se necessário, peça à segurança do prédio para subir ao andar, verificar e escoltar a pessoa para o andar correto (ele pode simplesmente ser de outra empresa e ter descido no andar errado).

Os pontos chaves deste capítulo são:

- A recepção INTERNA não deve abrir a porta para dar acesso ao escritório; Todos os visitantes devem ser acompanhados por um colaborador (normalmente o anfitrião), DESDE a recepção da Enauta;
- Não atendemos fornecedores da Enauta fora do local reservado para a recepção de fornecedores.

7. Penalidades

7.1. Violação das Políticas

A violação desta Política poderá acarretar sanções administrativas e/ou legais, sem prejuízo da rescisão do contrato de trabalho e/ou qualquer outro contrato de relacionamento de prestação de serviço entre o colaborador, associado, consultor e/ou sócio, assim como qualquer entidade com relação contratual direta ou indireta com a Enauta.

A observação do descumprimento desta política deve ser imediatamente reportada por meio do email: segurancasi@enauta.com.br

8. Vigência

Esta Política entrará em vigor a partir da data de sua aprovação pelo Conselho de Administração e permanecerá em vigor por prazo indeterminado.

9. Documentos de Referência

- Contrato de Trabalho;
- Código de Conduta;
- Política de Tratamento de Dados Pessoais
- ISO 27000
- Lei Geral de Proteção de Dados (Lei nº 13.709)