POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA ESSENTIA ENERGIA

A presente **Política de Segurança da Informação** ("PSI" ou "Política") apresenta os princípios gerais de conduta e as obrigações a serem seguidas pelos Colaboradores da ESSENTIA ENERGIA, incluindo todas as suas controladas e coligadas, marcas e divisões ("ESSENTIA"), a fim de mitigar eventuais riscos relacionados às ameaças externas ou internas, deliberadas ou acidentais, que possam impactar as informações da ESSENTIA quanto à sua integridade, autenticidade, confidencialidade e disponibilidade.

ÍNDICE

1. OBJETIVOS

O objetivo desta Política é orientar e estabelecer as diretrizes corporativas da ESSENTIA para a proteção dos ativos de informação e a prevenção de danos. Deve, portanto, ser cumprida e aplicada em todas as áreas e por todos os Colaboradores da ESSENTIA que, no âmbito da relação com a ESSENTIA, tiveram, tenham ou possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade da ESSENTIA, cujo acesso seja controlado.

2. DEFINIÇÕES

Para os efeitos desta Política, as seguintes definições terão os significados assinalados abaixo:

a) **Informações Protegidas:** todo e qualquer dado ou informação que o Colaborador desenvolva ou venha a ter acesso em virtude do seu vínculo com a ESSENTIA ou do desempenho de suas atividades contratadas pela ESSENTIA.

b) **Equipe de TI:** equipe de Tecnologia da Informação da ESSENTIA.

c) **Dados Pessoais:** informação relacionada a uma pessoa natural identificada ou identificável (p. ex.: nome, CPF, endereço, telefone celular e e-mail), incluindo eventuais dados sensíveis (dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico).

d) **Colaborador**: sócios, diretores, administradores, empregados, prestadores de serviços, representantes comerciais, parceiros e/ou quaisquer outros similares que tiverem acesso às dependências e às Informações Protegidas da ESSENTIA.

3. ESCOPO

Esta PSI é aplicável a toda ESSENTIA, contemplando todo o uso de dispositivos, acesso a servidores, conexões à rede e à internet e quaisquer outros usos de recursos tecnológicos ou que contenham informações da ESSENTIA. É obrigação de cada Colaborador manter-se atualizado em relação a esta PSI, bem como a procedimentos e normas relacionadas.

TODOS OS COLABORADORES DEVEM OBRIGATORIAMENTE CUMPRIR AS DISPOSIÇÕES EXPRESSAS NESTA POLÍTICA, INDEPENDENTEMENTE DE SEU CARGO, FUNÇÃO, ÁREA DE ATUAÇÃO OU LOCALIDADE NA QUAL EXERÇA SUAS ATIVIDADES VINCULADAS À ESSENTIA. O NÃO CUMPRIMENTO DAS DISPOSIÇÕES ORA PREVISTAS PODERÁ SUJEITAR O COLABORADOR INFRATOR ÀS SANÇÕES DISPOSTAS NO ITEM 19.

4. INFORMAÇÕES PROTEGIDAS

As Informações Protegidas são consideradas informações de exclusiva propriedade da ESSENTIA, salvo disposição diversa. Em relação a tais informações, é expressamente proibida a sua reprodução, divulgação, publicação, transmissão, cessão ou facilitação de acesso a quaisquer terceiros, direta ou indiretamente, total ou parcialmente, salvo se autorizado por esta Política ou, previamente e por escrito, pelos representantes legais da ESSENTIA.

Qualquer Informação Protegida cuja divulgação seja exigida por lei, ordem judicial, determinação de autoridades administrativas competentes ou acordos celebrados pela ESSENTIA com terceiros somente poderá ser divulgada após análise e validação da ESSENTIA, com o devido suporte jurídico.

A qualquer tempo, caso seja solicitado pela ESSENTIA, ou em caso de término da relação do Colaborador com a ESSENTIA, independentemente da causa, o Colaborador restituirá à ESSENTIA todas as cópias, bancos de dados, reproduções ou adaptações que porventura tiver realizado.

5. CLASSIFICAÇÃO DAS INFORMAÇÕES PROTEGIDAS

Para assegurar a proteção adequada das Informações Protegidas, é necessário que elas sejam classificadas de acordo com o impacto relacionado à quebra de confidencialidade , aplicando-se o grau de sigilo conforme sua classificação:

(i) **Informação Pública:** informação oficialmente liberada pela ESSENTIA para o público geral. A divulgação deste tipo de informação não tem potencial de causar problemas à ESSENTIA, podendo ser compartilhada livremente com o público geral, desde que seja mantida sua integridade.

(ii) **Informação Interna:** informação que guarda assuntos exclusivamente pertinentes à esfera interna da ESSENTIA, cujo acesso é liberado apenas às pessoas internas da ESSENTIA designadas para tal, bem como órgãos reguladores quando necessário. Embora a ESSENTIA não tenha interesse em divulgá-la a indivíduos externos, a disponibilização desse tipo de informação não tem o potencial de causar danos sérios à ESSENTIA ou a divulgação para órgãos públicos é necessária para garantir o cumprimento de obrigações regulatórias ou operacionais, como comunicações com ONS, ANEEL, CCEE, ANA, MME, entre outros;

(iii) **Informação Confidencial:** informação sigilosa que não deve ser divulgada. Seu uso é restrito a um determinado número de pessoas para desempenharem as suas atividades vinculadas à ESSENTIA. A sua divulgação não autorizada pode causar prejuízos para a ESSENTIA (tais como perda de clientes, danos financeiros, depreciação da imagem etc.), propiciando vantagens aos seus concorrentes e clientes, bem como revelando estratégias e resultados de negócios; e

(iv) **Informação Secreta**: informação sigilosa, com acesso controlado e liberado apenas às pessoas nomeadas para tanto, que contém matérias de ordem vital para a ESSENTIA ou seus clientes, cuja divulgação, inexatidão e indisponibilidade (total ou parcial) podem causar danos morais ou patrimoniais graves à ESSENTIA. Devem ser consideradas Informações Secretas as informações de saúde de Colaboradores (p. ex: exames médicos), os procedimentos de segurança e informações de notável criticidade para os negócios da ESSENTIA.

Caso o Colaborador receba uma informação que não esteja classificada, ele deve considerar, obrigatoriamente, essa informação como sendo, no mínimo, uma Informação Confidencial.

6. PRIVACIDADE E PROTEÇÃO DE DADOS

Esta PSI aplica-se a dados, incluindo Dados Pessoais, sobre clientes, Colaboradores e, quando pessoas físicas, consumidores finais de nossos clientes. É vedado, sem a prévia autorização da ESSENTIA, o uso destes dados para finalidades diversas das que motivaram a coleta, o uso, o armazenamento e qualquer outra hipótese de tratamento dos dados, nos termos desta Política, especialmente para fins particulares.

A ESSENTIA utiliza prestadores de serviço externos. Em caso de compartilhamento de Dados Pessoais com tais prestadores de serviço, devem ser firmados acordos contratuais apropriados e medidas técnicas e organizacionais de segurança devem ser implementadas de acordo com a legislação aplicável para assegurar a proteção dos dados.

O Colaborador deve atuar para garantir que todos os Dados Pessoais a que tiver acesso não sejam divulgados ou compartilhados sem autorização expressa da ESSENTIA, bem como não sejam transmitidos ou acessados por terceiros não autorizados. O Colaborador deve adotar as melhores práticas de segurança da informação durante todo o ciclo de vida dos Dados Pessoais dentro da ESSENTIA.

7. MONITORAMENTO E AUDITORIA DO AMBIENTE

TODO AMBIENTE FÍSICO E DIGITAL DA ESSENTIA DISPONIBILIZADO AOS COLABORADORES PODERÁ SER MONITORADO A QUALQUER MOMENTO, RESPEITADOS OS LIMITES PREVISTOS NA LEGISLAÇÃO VIGENTE, COM O OBJETIVO DE APURAR O CUMPRIMENTO DAS NORMAS E PROCEDIMENTOS DA ESSENTIA. SENDO ASSIM, OS DISPOSITIVOS DA ESSENTIA OU DISPONIBILIZADOS PELA ESSENTIA NÃO DEVEM SER UTILIZADOS PARA FINS PESSOAIS.

OS COLABORADORES DEVEM ESTAR CIENTES DE QUE A ESSENTIA PODERÁ:

(i) MONITORAR TODOS OS SERVIDORES, REDES, CONEXÕES DE INTERNET, SOFTWARES, EQUIPAMENTOS E DISPOSITIVOS CORPORATIVOS, MÓVEIS OU NÃO, CONECTADOS À REDE CORPORATIVA DA ESSENTIA; E

(ii) REALIZAR INSPEÇÕES FÍSICAS NOS EQUIPAMENTOS E NAS ESTAÇÕES DE TRABALHO DO COLABORADOR, PERIODICAMENTE OU SOB FUNDADA SUSPEITA DE INFRAÇÃO ÀS NORMAS INTERNAS DA ESSENTIA.

O Colaborador também está ciente de que o monitoramento poderá identificá-lo e apresentar dados sobre o uso da infraestrutura técnica da ESSENTIA e do material e conteúdo manipulado pelo Colaborador, sendo certo que todas as informações coletadas no curso do monitoramento são guardadas nos backups da ESSENTIA para fins de auditoria, inclusive aquelas coletadas no âmbito das gravações dos ramais dos Centros de Operações ou chamadas de rádio, e poderão ser utilizadas como provas de eventual violação das regras e condições estabelecidas pela ESSENTIA ou pela legislação em vigor. Caso solicitado pelos órgãos competentes, incluindo, mas não se limitando a, o Operador Nacional do Sistema Elétrico (ONS), essas informações poderão ser divulgadas na medida em que houver razão para tanto.

O Colaborador entende que o monitoramento é realizado para resguardar a segurança não só dos sistemas da ESSENTIA e das Informações Protegidas, como também do próprio Colaborador.

8. MANUSEIO DAS INFORMAÇÕES PROTEGIDAS

O Colaborador é responsável pelo uso que fizer das Informações Protegidas. Assim, as regras abaixo deverão ser observadas para garantir um nível mínimo de segurança:

- Utilize impressoras e copiadoras apenas para fins profissionais e retire os documentos imediatamente após o uso, especialmente se contiverem Informações Confidenciais;
- Evite deixar anotações ou Informações Protegidas em locais públicos ou de circulação, como salas de reunião, cafés ou aviões;
- Bloqueie o sistema operacional de sua estação de trabalho sempre que se ausentar, ainda que por curto período, a fim de prevenir o acesso não autorizado a dados pessoais, informações corporativas ou recursos tecnológicos.;
- Somente compartilhe Informações Protegidas com terceiros mediante contrato com cláusula de sigilo e, quando necessário, disposições sobre o uso adequado de Dados Pessoais;
- Arquivos enviados, recebidos ou compartilhados devem estar relacionados às atividades da ESSENTIA e não podem conter conteúdo ilegal, ofensivo ou que infrinja direitos de terceiros;
- Informações armazenadas fisicamente devem ser guardadas em locais seguros e trancados. Anotações e documentos não devem ficar expostos;
- Arquivos digitais devem ser salvos em diretórios restritos da rede corporativa. Caso sejam levados em dispositivos móveis, devem ser excluídos após o uso; e
- Alterações ou movimentações de arquivos confidenciais só devem ocorrer quando for possível garantir recuperação, versionamento ou rastreabilidade.

O descarte de um documento físico ou a exclusão de um arquivo digital que contenha Informações Protegidas deverá seguir as regras de descarte definidas pela Equipe de TI. No caso de informações que envolvam Dados Pessoais, o Colaborador seguirá os procedimentos descritos nas políticas ou normas internas aplicáveis.

9. CÓDIGOS MALICIOSOS

A ESSENTIA disponibiliza ferramentas para proteção dos seus ativos de informação e recursos computacionais, incluindo dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos tais como vírus, *worms*, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares.

No entanto, é importante ressaltar que a eficácia dessas soluções depende também do uso consciente e responsável por parte dos Colaboradores, que devem seguir as políticas internas de segurança da informação e boas práticas estabelecidas pela ESSENTIA. Sempre que apropriado, recomenda-se a consulta às políticas ou normas internas da ESSENTIA sobre o tema, que detalham os procedimentos de prevenção, testes e treinamentos destinados a reduzir riscos relacionados a ameaças digitais.

10. E-MAIL CORPORATIVO

Os endereços de e-mail fornecidos pela ESSENTIA aos Colaboradores são individuais e destinados exclusivamente para fins corporativos e relacionados às atividades do Colaborador dentro da ESSENTIA.

Adicionalmente, é proibido o uso de e-mail para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se autorizadas e relacionadas a uso legítimo da ESSENTIA;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente ou a ESSENTIA e as suas unidades vulneráveis a ações judiciais ou processos administrativos;
- divulgar informações não autorizadas, incluindo, sem limitação, imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo gestor responsável; e
- falsificar informações de endereçamento ou adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas.

11. INTERNET

A ESSENTIA visa o desenvolvimento de um comportamento ético e profissional no uso da internet. Para garantir a utilização racional desses recursos, bem como a segurança dos dados e softwares, a ESSENTIA se reserva o direito de utilizar ferramentas para verificar o conteúdo dos e-mails corporativos e monitorar o uso da internet e da rede corporativa realizada por Colaboradores, nos termos do item 7 desta Política.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá resultar em ações administrativas e penalidades decorrentes de processos civil e criminal, sendo que nesses casos a ESSENTIA cooperará ativamente com as autoridades competentes.

Os Colaboradores com acesso à internet poderão fazer o download somente de softwares ligados diretamente às suas atividades na ESSENTIA e deverão providenciar o que for necessário para regularizar a licença e o registro desses softwares, sempre buscando a aprovação da Equipe de TI.

12. REDES SOCIAIS E E-MAIL PESSOAL

A ESSENTIA poderá suspender, sem aviso prévio e a seu exclusivo critério, o uso e o acesso a redes sociais, e-mails pessoais e serviços de mensagens para fins pessoais, nas dependências físicas e nos dispositivos da ESSENTIA, por questões de governança e de segurança da informação.

13. ACESSO À REDE DE ARQUIVOS

13.1. ACESSO FÍSICO ÀS INFORMAÇÕES

Os locais onde estão armazenados os arquivos físicos da ESSENTIA são considerados parte crítica da sua infraestrutura tecnológica, razão pela qual o cuidado com a proteção e segurança deve ser obrigatoriamente redobrado. Há diferentes tipos de acessos e, para cada, diferentes regras e restrições, conforme consta abaixo:

(i) **acessos permanentes:** permitidos somente aos Colaboradores da ESSENTIA que tenham a necessidade de acesso liberado a tais locais para executar suas atividades;

(ii) **acessos esporádicos**: permitidos a outros Colaboradores ou a visitantes externos, mediante autorização prévia da ESSENTIA, e desde que haja acompanhamento em tempo integral pela equipe responsável; e

(iii) **acessos externos:** permitidos àqueles que não sejam Colaboradores da ESSENTIA, mediante

autorização e desde que tenham contrato vigente com a ESSENTIA que justifique tal acesso.

13.2. ACESSO LÓGICO

O acesso às informações armazenadas na infraestrutura tecnológica da ESSENTIA é restrito a cada Colaborador, a depender do perfil de acesso que lhe for atribuído. Cada perfil pressupõe a liberação do acesso de determinados diretórios dentro da rede da ESSENTIA, de modo que as informações poderão ser acessadas de acordo com o nível de acesso definido pela ESSENTIA.

13.3. ACESSO REMOTO

Quando o Colaborador não se encontrar nas dependências da ESSENTIA, o Colaborador poderá acessar o e-mail corporativo, rede e outros documentos da ESSENTIA de forma remota, conforme o regime de trabalho adotado. No caso do regime de trabalho híbrido, o acesso remoto é previamente configurado pela Equipe de TI no equipamento do colaborador.

O acesso remoto somente é permitido para execução das atividades profissionais do Colaborador que estejam vinculadas à ESSENTIA, de forma que tal acesso não poderá ser realizado por dispositivo ou software particulares do Colaborador ou de propriedade de terceiros, exceto se autorizado. O Colaborador é responsável por todas as atividades realizadas quando do seu acesso remoto, respondendo por qualquer uso irregular, inclusive por outra pessoa na posse de seu acesso. No caso de furto, roubo ou extravio de equipamento móvel que tenha o acesso remoto às Informações Protegidas da ESSENTIA, o Colaborador deverá imediatamente comunicar o fato à Equipe de TI.

14. IDENTIFICAÇÃO E SENHAS

Todos os Colaboradores têm determinados privilégios de acesso a Informações Protegidas, de acordo com seu cargo e as suas atribuições. Alguns exemplos de privilégio são o acesso externo ao e-mail, liberações no acesso à Internet e no acesso lógico, utilização externa de determinados equipamentos da ESSENTIA, liberação de espaço em disco rígido, utilização de dispositivos móveis, entre outros.

O Colaborador receberá um login e uma senha, de acordo com o perfil que lhe for atribuído, que lhe permitirá ser identificado quando do acesso à infraestrutura da ESSENTIA. Assim, o Colaborador somente terá acesso às áreas da infraestrutura da ESSENTIA que forem autorizadas considerando o seu perfil. A ESSENTIA reserva-se o direito de revisar, a qualquer momento e sem aviso prévio, os privilégios de qualquer Colaborador, a fim de resguardar os níveis de segurança da informação da ESSENTIA.

O login e a senha do Colaborador são individuais, intransferíveis e, consequentemente, o Colaborador é o responsável pelo sigilo e pela manutenção segura da sua senha vinculada ao login, sendo proibido o compartilhamento de login e senha com terceiros, inclusive outros Colaboradores, sob pena de arcar com as sanções não só previstas nesta Política, mas também as penalidades civis, criminais e trabalhistas, respondendo, inclusive, por todo e qualquer dano que causar à ESSENTIA. O Colaborador deve tomar as devidas medidas para manutenção do sigilo das senhas de acesso concedidas, de modo que não deve anotar ou registrar senhas de acesso em locais expostos, tais como embaixo do teclado ou do monitor, em *post-its* etc.

15. DISPOSITIVOS

Os dispositivos físicos capazes de armazenar Informações Protegidas, como computadores, celulares, notebooks, tablets e outros, disponibilizados aos Colaboradores para a execução de suas atividades, são de propriedade da ESSENTIA, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da ESSENTIA.

Os equipamentos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos. Os computadores devem ter o recurso de atualizações automáticas do sistema operacional habilitada por padrão e software antivírus instalado, ativado e atualizado frequentemente.

Arquivos pessoais ou não pertinentes ao negócio da ESSENTIA (fotos, músicas, vídeos e outros arquivos não

relacionados ao trabalho) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento no disco do computador. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente.

Documentos imprescindíveis para as atividades dos Colaboradores deverão ser salvos em diretório sincronizado com o serviço de Cloud, garantindo o backup e a disponibilidade por meio de qualquer computador. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio Colaborador.

O Colaborador entende que é o responsável por todo e qualquer dano que causar nos equipamentos, por dolo ou culpa, e está ciente e concorda em observar as regras do Anexo I. O uso indevido dos dispositivos da ESSENTIA sujeitará o Colaborador às sanções aplicáveis, conforme indicado no item 19, a depender da gravidade da conduta praticada.

16. DATA CENTER E SERVIÇOS DE ARMAZENAMENTO EM NUVEM (CLOUD)

A ESSENTIA utiliza, no curso de suas operações, softwares próprios e de terceiros. O Colaborador compromete-se a observar integralmente as responsabilidades descritas no Anexo I, referentes à utilização adequada desses softwares.
A ESSENTIA disponibiliza serviços de Cloud para o armazenamento externo de arquivos, software e sistemas. Assim, é proibido a utilização pelo Colaborador de serviços de armazenamento na nuvem não disponibilizados por meio da infraestrutura tecnológica da ESSENTIA.

17. DESLIGAMENTO OU MOVIMENTAÇÃO DO COLABORADOR

Ao término do vínculo do Colaborador com a ESSENTIA, o seu acesso à infraestrutura tecnológica da ESSENTIA será revogado de forma imediata. O Colaborador deverá devolver todos e quaisquer dispositivos de propriedade da ESSENTIA que estejam em sua posse, em perfeitas condições de uso, juntamente com eventuais acessórios que lhe tenham sido entregues. As obrigações de sigilo e não reprodução das Informações Protegidas assumidas pelo Colaborador nessa PSI permanecerão em vigor mesmo após o desligamento do Colaborador.

Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento à ESSENTIA. Caso o Colaborador tenha acesso à conta de e-mail corporativa ou a qualquer outro software corporativo instalado em um dispositivo pessoal, deverá imediatamente desinstalá-los.

Caso o Colaborador mude de departamento ou de função dentro da ESSENTIA, também deverá haver uma revisão dos acessos, de modo que o Colaborador visualize apenas os sistemas e pastas de rede necessários ao desempenho de sua nova função.

18. REPORTE DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Para evitar a exposição indevida das Informações Protegidas, a ESSENTIA emprega medidas de segurança, tanto internas quanto externas, as quais atendem as obrigações legais vigentes. Porém, essas medidas somente serão eficazes se o Colaborador cumprir com as obrigações de segurança assumidas nesta Política.

Caso o Colaborador tome conhecimento ou suspeite de qualquer acontecimento que viole as regras desta Política ou coloque em risco a segurança das informações da ESSENTIA, o Colaborador deverá imediatamente comunicar a ESSENTIA, que irá apurar as causas e os efeitos do incidente ocorrido, para então tomar as medidas de contenção, avaliação de impacto e necessidade de comunicação sobre o incidente ao órgão competente e/ou aos titulares das Informações Protegidas, conforme a Política de Reposta a Incidentes da ESSENTIA.

19. SANÇÕES

Caso o Colaborador não cumpra as regras desta Política, estará sujeito à aplicação de sanções de acordo com o grau de gravidade da conduta praticada pelo Colaborador, podendo variar entre:

(i) **advertência:** no caso de infrações consideradas leves;

(ii) **suspensão:** no caso de infrações consideradas graves ou quando for constatada a reincidência de uma conduta classificada leve; e

(iii) **encerramento do contrato:** no caso de infrações consideradas gravíssimas ou quando for constatada reincidência de uma conduta considerada grave. Tratando-se de Colaborador empregado, isso significa o desligamento do Colaborador e a rescisão de seu contrato de trabalho por justa causa.

Os Colaboradores que cometerem infração às regras desta Política serão comunicados por escrito. Tal comunicação conterá a regra violada, a conduta praticada pelo Colaborador e a sanção aplicada pela ESSENTIA, sem prejuízo de eventual indenização, a ser apurada judicialmente.

20. ATUALIZAÇÃO DESTA POLÍTICA

Essa Política poderá ser revista, atualizada e alterada a qualquer tempo, a exclusivo critério da ESSENTIA, sempre que algum fato relevante ou evento motive sua revisão antecipada. Em caso de dúvidas, comentários ou sugestões relacionadas a esta Política, favor entrar em contato pelos e-mails patricia.levy@essentiaenergia.com.br e ti@essentiaenergia.com.br

Histórico de Atualizações:

Versão	Data	Descrição da Alteração	Revisado por	Aprovado por

21. ELABORAÇÃO DESTA POLÍTICA

Responsáveis:

Nome	Cargo	Função	Assinaturas
Patricia de Araujo Levy	Gerente Executiva Jurídica e Diretora	Elaboração, Revisão e Aprovação	DocuSigned by: Patrícia de Araujo Levy 1693328762FE469...
Adrisson Floriano	Gerente de Tecnologia IT & OT	Elaboração e Revisão	Signed by: Adrisson Floriano C1F67E962241431...
Gilberto Luis Peixoto dos Santos Filho	COO	Revisão e Aprovação	Assinado por: C08C474BC0CC42A...

ANEXO I- RESPONSABILIDADES

Visando a integridade e disponibilidade dos ativos e sistemas da ESSENTIA, os Colaboradores têm algumas responsabilidades que devem ser observadas. Abaixo, seguem as respectivas responsabilidades dos Colaboradores da ESSENTIA em relação à Política de Segurança da Informação:

a) RESPONSABILIDADES GERAIS

- Observar as disposições de segurança da informação presentes na Política;
- Encaminhar quaisquer dúvidas sobre a Política suas normas e procedimentos para os canais indicados na Política;
- Manter sigilo sobre todas as informações que venha a tomar conhecimento em virtude das suas atividades profissionais, inclusive após o término da relação contratual existente, a qualquer título, por qualquer das partes;
- Zelar e manter em segurança suas credenciais e senhas de acesso aos sistemas de informação; e
- Comunicar qualquer evento que viole a Política ou possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da ESSENTIA.

b) SOFTWARES

- Não utilizar os softwares da ESSENTIA para fins pessoais ou de qualquer forma que comprometa a segurança da infraestrutura da ESSENTIA;
- Não excluir, modificar, copiar, transferir, realizar engenharia reversa ou ceder o acesso de tais softwares a terceiros, ou praticar qualquer ato que esteja em desacordo com a legislação aplicável;
- Não instalar na rede ou nos dispositivos da ESSENTIA qualquer software pirata, não licenciado ou não autorizado, sendo que qualquer software não autorizado que seja baixado pelo Colaborador deverá ser excluído; e
- Não utilizar softwares *peer-to-peer* (BitTorrent, por exemplo) ou cujo serviço oferecido seja o de *streaming* (por exemplo, músicas, vídeos, filmes e rádio online).

c) EQUIPAMENTOS

- Empregar todos os cuidados necessários ao utilizar os equipamentos da ESSENTIA;
- Informar qualquer identificação de dispositivo estranho conectado ao seu computador;
- Manter a configuração do equipamento disponibilizado pela ESSENTIA, seguindo os devidos controles de segurança exigidos pela Política e pelas normas específicas da ESSENTIA, assumindo a responsabilidade como custodiante de informações;
- Alterar senhas padrões (*default*) de todos os recursos tecnológicos aos quais fizer uso;
- Não deixar os dispositivos logados quando não estiver perto do equipamento;
- Comunicar os gestores se, no decorrer do uso do seu dispositivo, o Colaborador tiver dúvidas sobre o seu manuseio ou constatar falhas que impliquem na necessidade de substituição ou manutenção;
- Devolver os equipamentos para a ESSENTIA em perfeitas condições de uso, juntamente com eventuais acessórios lhe tenham sido entregues, como bolsas, *cases*, películas etc., tão logo termine o período necessário para o uso;
- Comunicar imediatamente a ESSENTIA no caso de perda, furto, roubo ou dano ao equipamento;
- Não deixar dispositivos em locais públicos, em veículos ou em qualquer outro local fora das dependências da ESSENTIA em que possa haver acesso ao equipamento por pessoas não autorizadas, a fim de evitar o furto ou roubo destes equipamentos, bem como o vazamento das Informações Protegidas nele contidas; e
- Não abrir, manusear ou proceder ao reparo dos computadores ou outros equipamentos de informática junto a um técnico de informática que não seja da ESSENTIA ou que não tenha sido devidamente contratado pela ESSENTIA.

d) SENHA

- Respeitar integralmente as diretrizes estabelecidas nas políticas ou normas internas sobre o tema.

e) CÓDIGOS MALICIOSOS

- Respeitar integralmente as diretrizes estabelecidas nas políticas ou normas internas sobre o tema,

observando os procedimentos de prevenção, detecção e resposta a tentativas de fraude eletrônica.

***