POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DEZEMBRO 2020

INFORMAÇÕES PRELIMINARES

Responsável pela área: Dymythro Mitchell Fernandes de Souza
Período: Dezembro 2020 – Dezembro 2021
Classificação: Público
Confidencial – Restrito – Público

Próxima Revisão: Se houver mudanças na legislação ou necessidade interna da empresa

CARACTERÍSTICAS DO PROCESSO

Área de Aplicação: Todos os Colaboradores (Próprios e Terceiros) sejam pessoas físicas ou jurídicas, tais como, mas não limitados a associações, diretores, fornecedores, subcontratados, despachantes, consultores, prestadores de serviços, entre outros.

Áreas envolvidas: Todas
Interfaces do processo

Unidades de aplicação: Matriz e Filiais - Brasil

Legislação Aplicável: Resolução BACEN nº 4658 de 26 de abril de 2018, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil;

Lei nº 13.709/2018, que dispõe sobre a proteção de dados pessoais;

Lei nº 12.965 de 23 de abril de 2014 – Marco Civil da Internet;

Lei nº 12.527 de 18 de novembro de 2011, que dispõe sobre o acesso à informação;

ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.

A empresa **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**, pessoa jurídica, inscrita no **CNPJ 02.371.211/0001-66**, com sede na SRTVS Quadra 701 Conjunto L Número 38 Bloco 1 Sala 305, Edifício Assis Chateaubriand, Brasília - DF, **DECLARA**, para os devidos fins que se compromete a atuar exclusivamente dentro do escopo da lei aplicável em vigor e que:

Assume que é expressamente contrária à prática de atos lesivos à administração pública, assim entendidos todos aqueles atos que atentem contra o patrimônio público, contra os princípios da administração pública ou contra os compromissos aqui assumidos.

CARTA DE COMPROMETIMENTO DA ALTA DIREÇÃO

A efetividade Política de Segurança da Informação depende estritamente do comprometimento da alta direção. É essencial que os responsáveis por liberar recursos, aplicar sanções, criar regras e portarias, apoiem a PSI e demonstrem seu comprometimento para que os colaboradores se sintam motivados a cumpri-la

ELONET

CARTA DE COMPROMETIMENTO DA ALTA DIREÇÃO

A **ELONETH** acredita que a informação é um dos principais bens de qualquer organização. Assim, estabelece sua Política de Segurança da Informação, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações e de propriedade intelectual da empresa, dos clientes, dos parceiros e do público em geral.

A fim de dar mais um passo em busca da concretização de seus padrões éticos, a **ELONETH** assinou sua Política de Segurança da Informação, comprometendo-se com isso a propagar a lei geral de proteção de dados para seus colaboradores e clientes, para que esta possa ser cada vez mais conhecida e cumprida.

Este passo importante, qual seja a assinatura da sua Política de Segurança da Informação, não é novo, e vem sendo construído pela **ELONETH** há anos, com a implementação de programas de gestão e práticas de Compliance de mercado.

Diante da concretização da sua Política de Segurança da Informação, a **ELONETH** agradece a cada um dos seus colaboradores e clientes pelo empenho, e acredita na estrita observância deste Código por todos.

Ítalo Oliveira Torres
Eloneth Habitação Cons. Asses. Empresarial Ltda

Elonet Habitação Ltda
www.elonethabitacao.com.br
MATRIZ: Fone/Fax (61) 3225-3845

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

OBJETIVO

A presente **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** é uma declaração formal da ELONETH acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, em total conformidade com as leis estabelecidas e os regulamentos aplicáveis, visando assim garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização de negócio da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**

A alta administração tem a responsabilidade de divulgar e assegurar o cumprimento das determinações desta **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** que ferem os princípios desta Política.

APLICAÇÃO

Esta Politica aplica-se a a todos os funcionários e contratados da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA** no que se refere a trabalhar nas instalações da empresa ou negócios da mesma, que de agora em diante será referido como colaborador.

Esta política foi elaborada pensando na melhor forma de orientar nossos colaboradores, para que possamos ter uma empresa que seja exemplo de transformação de valores no mercado de construção civil, obras de infraestruturas e serviços.

OS NOSSOS VALORES

MISSÃO: Prestar consultoria e assessoria especializada, valorizando as necessidades individuais de cada cliente

VISÃO: Se manter entre as melhores empresas do ramo e no atendimento aos seus clientes, numa busca crescente pela qualidade e de novas tecnologia para o tratamento da informação, investindo e proporcionando um ambiente favorável ao trabalho em equipe, para uma melhor eficácia organizacional.

VALORES: Manter relacionamento com seus clientes de forma clara e confiável, baseado na ética e confiança mútua, prestação de serviços de qualidade e apresentação de soluções inovadoras, sempre buscando o melhor resultado.

DAS RESPONSABILIDADES

1 – Colaboradores

Será de inteira responsabilidade de funcionários, terceirizados e demais colaboradores da ELONETH:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da ELONETH;
- Buscar o Setor de Informática para esclarecimentos de dúvidas referentes à PSI;
- Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pela ELONETH;
- Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela ELONETH;
- Descarte adequado de documentos de acordo com seu grau de classificação;
- Comunicar prontamente à chefia imediata qualquer violação a esta política, suas normas e

procedimentos.

2 – Setor de Recursos Humanos

Em relação à segurança da Informação, cabe ao setor de recursos humanos:

- Aprovar a Política de Segurança da Informação e suas atualizações;
- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da PSI da ELONETH;
- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
- Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;
- Elaborar, com o apoio do Setor de Informática, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;
- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;
- Tomar as decisões administrativas referentes aos descumprimentos da PSI da ELONETH

3 – Setor de Informática

Cabe ao Setor de Informática

- Propor melhorias, alterações e ajustes da PSI;
- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;
- Classificar e reclassificar o nível de acesso às informações sempre que necessário;
- Avaliar incidentes de segurança e propor ações corretivas;
- Definir as regras para instalação de software e hardware na ELONETH;
- Homologar os equipamentos pessoais (smartphones e notebooks) para uso na rede da ELONETH
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;
- Mediante informações do Setor de Recursos Humanos, manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;
- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades, etc.;
- Promover, com o envolvimento do Setor de Recursos Humanos, palestras de conscientização dos colaboradores em relação à importância da segurança da informação para o negócio da ELONETH;

Esta política não substitui as normas legais e sua leitura e assimilação é dever de todo o colaborador. Cada gestor (líder, supervisor, gerente, diretor) garantirá a execução dos procedimentos, assegurando o livre acesso ao termo escrito e à divulgação dos princípios aqui regulados. Caso uma situação não esteja clara, peça ajuda antes de agir. A chefia imediata é o caminho indicado para o aconselhamento.

A VIOLAÇÃO DESTA POLÍTICA DE SEGURANÇA É QUALQUER ATO QUE:

- Exponha a Empresa a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

É DEVER DE TODOS DENTRO DA ELONET HABITAÇÃO LTDA:

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA** e deve sempre ser tratada profissionalmente.

01 – CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

1 – Pública

2 – Interna

3 – Confidencial

4 – Restrita

Conceitos:

Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence.

A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

02 – DADOS PESSOAIS DE FUNCIONÁRIOS

A **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA** se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução do seu negócio.

Todos os Dados Pessoais de Funcionários serão considerados dados confidenciais.

Dados Pessoais de Funcionários sob a responsabilidade da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA** não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**.

03 – PROGRAMAS ILEGAIS

É terminantemente proibido o uso de programas ilegais (PIRATAS) na **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**. Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da Empresa.

Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

04 – PERMISSÕES E SENHAS

Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da Empresa, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de Informática, por meio de e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos. A Informática fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada a cada 45 (quarenta e cinco) dias, não podendo repetir a anterior.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

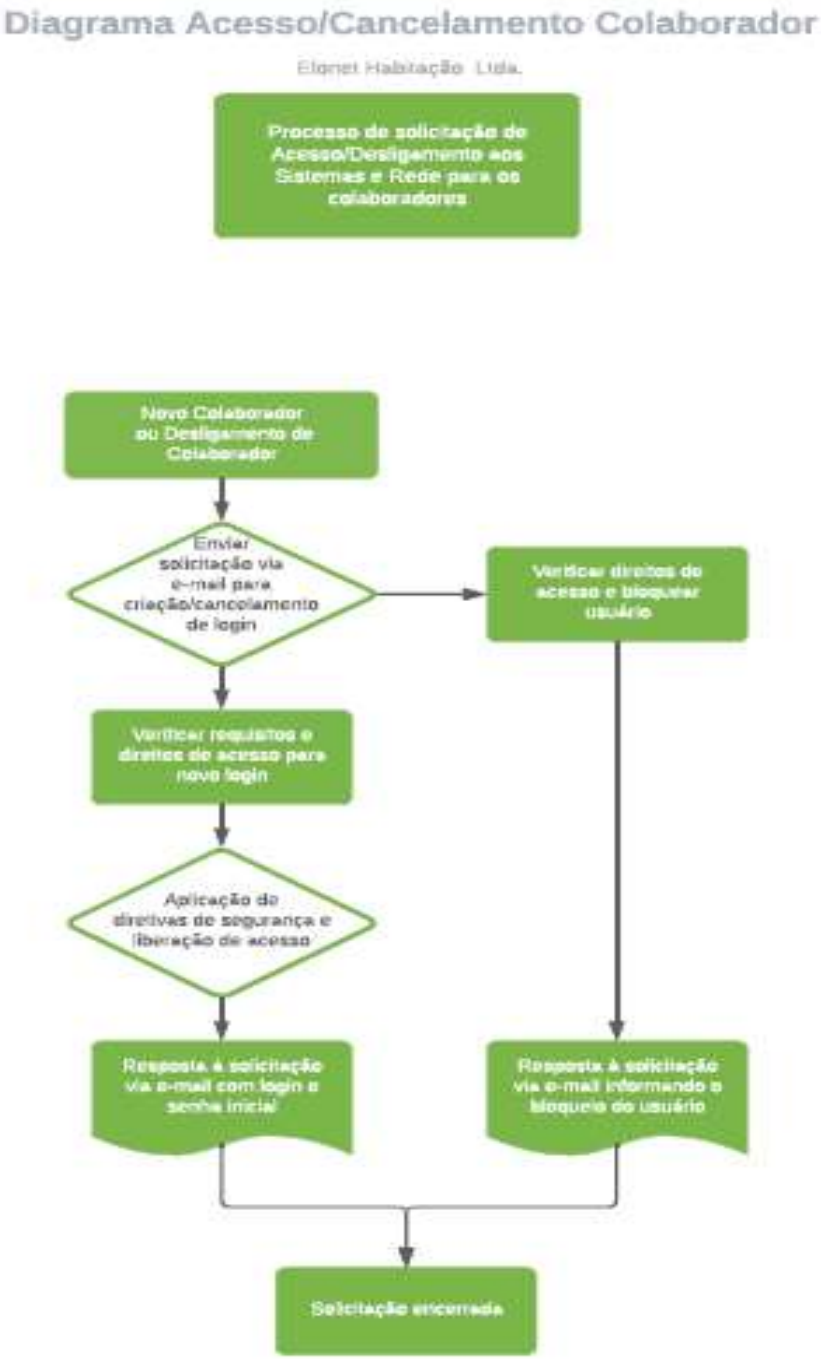
Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

1) A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;
2) A senha inicial só será fornecida ao próprio colaborador, pessoalmente. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;
3) É proibido o compartilhamento de login para funções de administração de sistemas;
4) As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);
5) As senhas deverão seguir os seguintes pré-requisitos:
    a. Tamanho mínimo de oito caracteres;
    b. Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;
    c. Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome

do cônjuge, etc).

6) O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:
   a. Desligamento do colaborador;
   b. Mudança de função do colaborador;
   c. Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.
7) Para os cancelamentos acima mencionados, o Setor de Recursos Humanos ficará responsável por informar prontamente o Setor de Informática acerca dos desligamentos e mudança de função dos colaboradores.

Controle de acesso lógico – Workflow



05 – COMPARTILHAMENTO DE PASTAS E DADOS

É de obrigação dos usuários rever periodicamente todos os compartilhamentos existentes em suas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos.

06 – CÓPIA DE SEGURANÇA (BACKUP) DOS SISTEMAS INTEGRADOS E SERVIDORES DE REDE

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra caso um incidente de perda de dados venha a ocorrer.

Cópias de segurança dos sistemas integrados e servidores de rede são de responsabilidade da Informática e deverão ser feitas diariamente.

Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, dos Sistemas Integrados. Estas cópias serão feitas imediatamente após a comunicação formal das áreas responsáveis, por meio de e-mail, que o referido mês foi encerrado.

O backup deverá obrigatoriamente abranger log de sistemas, servidores e rede.

O backup deve ser criptografado com AES256, estes deverão ser testados mensalmente.

O RESTORE só deve acontecer mediante autorização do gerente de TI.

07 – SEGURANÇA E INTEGRIDADE DOS BANCOS DE DADOS

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de Informática, assim como a manutenção, alteração e atualização de equipamentos e programas.

Fica terminantemente proibido o uso de dados de produção em ambiente de desenvolvimento, teste e homologação, bem como qualquer tipo de transferência desses dados ou parte dos mesmos entre tais ambiente.

Fica terminantemente proibido a exclusão, alteração ou desativação de log de sistemas, redes e equipamentos, inclusive por parte dos administradores.

Toda e qualquer modificação e exclusão de informações na aplicação WEB deverá ter log.

O registro de log do período de 1 ano deverá ficar disponível para acesso imediato, ou seja disponível para pronta análise.

08 – ADMISSÃO/DEMISSÃO DE FUNCIONÁRIOS/TEMPORÁRIOS/ESTAGIÁRIOS

O setor de Recrutamento e Seleção de Pessoal da Empresa deverá informar ao setor de Informática, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no domínio da Empresa. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo setor de Informática.

Cabe ao setor solicitante da contratação a comunicação ao setor de Informática sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser

informado o tempo em que o mesmo prestará serviço a Empresa, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.

No caso de demissão, o setor de Recursos Humanos deverá comunicar o fato o mais rapidamente possível à Informática, para que o funcionário demitido seja excluído do sistema.

No caso de afastamento, licença ou férias, o setor de Recursos Humanos deverá comunicar o fato o antecipadamente ao Setor de Informática, para que o colaborador em questão tenha seu acesso ao sistema suspenso durante esse período.

Mensalmente o Setor de Recursos Humanos enviará ao Setor de informática relatório informando o status de cada colaborador: Ativo, Férias, Afastamento, Demitido, etc.

Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**. Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

09 – TRANSFERÊNCIA DE FUNCIONÁRIOS

Quando um funcionário for promovido ou transferido de seção ou gerência, o Setor de Recursos Humanos deverá comunicar o fato ao Setor de Informática, para que sejam feitas as adequações necessárias aos sistemas informatizados da Empresa.

10 – CÓPIAS DE SEGURANÇA DE ARQUIVOS INDIVIDUAIS

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA** o Setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

11 – PROPRIEDADE INTELECTUAL

É de propriedade da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**, todas as criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a Empresa.

12 – USO DO AMBIENTE WEB

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na ELONET HABITAÇÃO LTDA. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

O uso da Internet será monitorado pelo Setor de Informática, inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da Direção da Empresa, com base em recomendação do Supervisor de Informática.

Não é permitido instalar programas provenientes da Internet nos microcomputadores da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**, sem expressa anuência do setor de Informática.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gerente da área requisite formalmente ao Setor de informática.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais; que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**;
- Que promovam discussão pública sobre os negócios da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível “Confidencial”;
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

13 – USO DO CORREIO ELETRÔNICO

O correio eletrônico fornecido pela **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA** é um instrumento de comunicação interna e externa para a realização do negócio da Empresa.

As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**, não podem ser contrárias à legislação vigente e nem aos princípios éticos da Empresa.

Fica **terminantemente proibido** o envio de dados/informações, em sua totalidade ou parcial, de clientes através de qualquer tipo de mensagem eletrônica, inclusive e-mail.

O acesso a e-mail pessoal é vedado dentro das dependências da ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA, mesmo que seja em equipamento pessoal, ou fora do horário de trabalho.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;

- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**.

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo.

A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado.

Não será permitido o uso de e-mail gratuitos (liberados em alguns sites da web), nos computadores da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**.

O Setor de Informática poderá, visando evitar a entrada de vírus na **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA**, bloquear o recebimento de e-mails provenientes de sites gratuitos.

14 – NECESSIDADES DE NOVOS SISTEMAS, APLICATIVOS E/OU EQUIPAMENTOS

O Setor de Informática é responsável pela aplicação da Política da **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA** em relação a definição de compra e substituição de “software” e “hardware”.

Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo Setor de Informática.

Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

15 – USO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

1) É de responsabilidade do colaborador do equipamento zelar pelo mesmo, mantendo-o em boas condições;
2) Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;
3) É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe do Setor de Informática;
4) As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas.
5) É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe do Setor de Informática;
6) É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe do Setor de Informática;

7) Todos os equipamentos devem ser posicionados de forma que o ângulo de visão seja restrito;
8) As estações de trabalho possuem bloqueio automático após 10 minutos de inatividade;
9) As estações de trabalho devem permanecer bloqueadas (logoff) nos períodos de ausência do colaborador;
10) Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
11) Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;
12) É proibido o uso de estações de trabalho para:
    a. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
    b. Burlar quaisquer sistemas de segurança;
    c. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    d. Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
    e. Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
13) O Setor de Informática não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da instituição;
14) As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

16 – USO DE COMPUTADORES PESSOAIS DE PROPRIEDADE DA ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA.

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade da ELONET HABITAÇÃO LTDA, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi etc.;
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;

- Atenção ao transportar o equipamento na rua.

Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao Setor de Informática;
- Envie uma cópia da ocorrência para o Setor de Informática.

17 – RESPONSABILIDADES DOS GERENTES/SUPERVISORES

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da Empresa, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O Setor de Informática fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Que informação ou rotina, determinado usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

18 – USO DE ANTI-VÍRUS

Todo arquivo em mídia proveniente de entidade externa a **ELONETH - HABITAÇÃO, CONSULTORIA E ASSESSORIA EMPRESARIAL LTDA** deve ser verificado por programa antivírus.

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.

Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

19 – NORMA DE SEGURANÇA DA DESCARTE DE INFORMAÇÕES

ABNT 16167-2013

Segundo a norma 16167-2013 Pág. 11 Tabela 2

Cenários	Pública	Interna	Confidencial	Restrita
Eliminação de mídia digital analógica	Sem restrição	Somente dentro das áreas da Organização	Convém que os dispositivos que contenham informações sensíveis sejam destruídos fisicamente ou as informações sejam destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis, em vez de usarem as funções-padrão de apagar ou formatar	Convém que os dispositivos que contenham informações sensíveis sejam destruídos fisicamente ou as informações sejam destruídas, apagadas ou sobregravadas por meio de técnicas que tomem as informações originais irrecuperáveis, em vez de usarem as funções-padrão de apagar ou formatar

Segundo a norma 16167-2013 Pág. 11 Tabela 2

Cenários	Pública	Interna	Confidencial	Restrita
Eliminação de mídia impressa	Sem restrição	Convém que a fragmentação seja realizada nas dependências da Organização	Convém que a fragmentação seja realizada nas dependências do setor responsável pela informação, quando possível, ou na presença de alguém do grupo de acesso ou do custo diante da informação	Convém que a fragmentação seja realizada nas dependências do setor responsável pela informação, quando possível, ou na presença de alguém do grupo de acesso ou do custo diante da informação

Segundo a norma 16167-2013 Pág. 12 Tabela 2

Cenários	Pública	Interna	Confidencial	Restrita
Eliminação de arquivos de computador	Sem restrição	Excluir da pasta onde está arquivada	Excluir da pasta onde está arquivada e da lixeira também	Excluir da lixeira dos dispositivos e adotar soluções tecnológicas visando garantir que as informações não possam ser recuperadas

NOTA 1: Informações menos críticas tem menos controles, ao passo que informações mais sensíveis tem maiores controles e restrições. Um exemplo tradicional é a eliminação de informações físicas. Informações que podem ser divulgadas publicamente não tem restrições quanto à eliminação, enquanto informações sensíveis devem ser fragmentadas.

NOTA 2: Convém que procedimentos complementares, quanto ao tratamento da informação, sejam considerados e desenvolvidos conforme apontado na norma ABNT NBR ISO lEC 27002:2005, Seção 10.7.

NOTA 3: Convém que sejam definidos procedimentos específicos de tratamento da informação onde a aplicação do rótulo não for possível, como por exemplo o uso de metadados, conforme ABNT NBR ISSO IEC 27002 Seção 7.2.2.

NOTA 4: Convém que sejam definidos pela Organização processos disciplinares adequados para aplicar no tratamento dos desvios realizados pelas pessoas em relação às diretrizes desta Norma, conforme ABNT NBR ISO lEC 27002, Seção 8.2.3.

NOTA 5: Convém que todos os funcionários, fornecedores e terceiros que tenham acesso a informações sensíveis assinem um termo de confidencialidade ou de não divulgação antes de lhes ser dado o acesso aos recursos de processamento da informação.

20 – REUTILIZAÇÃO E ALIENAÇÃO SEGURA DE EQUIPAMENTOS

Utilizando como referência a ABNT NBR 150 – ISSO IEC 27002-2005.

Segundo a norma 27002-2005, pag. 39 – 9.2.6:

- **Controle:** Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

- **Diretrizes para Implementação:** Convém que os dispositivos que contenham informações sensíveis sejam destruídos fisicamente ou as informações sejam destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis, em vez de se usarem as funções-padrão de apagar ou formatar.

- **Informações Adicionais**

    - No caso de dispositivos defeituosos que contenham informações sensíveis, pode ser necessário uma análise/avaliação de riscos para determinar se convém destruir fisicamente o dispositivo em vez de enviá-lo para o conserto ou descartá-lo.
    - As informações podem ser comprometidas por um descarte feito sem os devidos cuidados ou pela reutilização do equipamento;
    - Processos segundo a Norma 27002-2005 Pag 51-10.7.2.

Descarte de mídias

- **Controle:** Convém que as mídias sejam descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.

- **Diretrizes para implementação:**

    - Convém que procedimentos formais para o descarte das mídias sejam definidos para minimizar o risco de vazamento de informações sensíveis para pessoas não autorizadas.

- Convém que procedimentos para descarte seguro das mídias contendo informações sensíveis sejam relativos ao grau de sensibilidade das informações.

- **Convém que os seguintes itens sejam considerados:**
  - mídias contendo informações sensíveis que sejam guardadas e destruídas de forma segura e protegida, como, por exemplo, através de incineração ou trituração, ou da remoção dos dados para uso por uma outra aplicação dentro da organização;
  - procedimentos que sejam implementados para identificar os itens que requerem descarte seguro;
  - fáceis de implementar a coleta e descarte seguro de todas as mídias a serem inutilizadas, ao invés de tentar separar apenas aquelas contendo informações sensíveis;
  - muitas organizações oferecem serviços de coleta e descarte de papel, de equipamentos e de mídias magnéticas;
  - que se tenha o cuidado na seleção de um fornecedor com experiência e controles adequados;
  - descarte de itens sensíveis seja registrado em controles, sempre que possível, para se manter uma trilha (ou linha) de auditoria.
  - Quando da acumulação de mídias para descarte, convém que se leve em consideração o efeito proveniente do acúmulo, o que pode fazer com que uma grande quantidade de informação não sensível torne-se sensível.
- **Informações adicionais**
  - Informações sensíveis podem ser divulgadas através do descarte negligente das mídias (ver 9.2.6 para informações de descarte de equipamentos).

21 – PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: Advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

DISPOSIÇÕES FINAIS

É responsabilidade de cada colaborador assegurar o cumprimento dos termos dispostos nesta política. Os Gerentes têm o dever de ser o exemplo e disseminar o conteúdo aqui exposto. Incentivamos a comunicação de qualquer prática que possa representar violação desta política, em especial fraudes e corrupção, ou ainda atos que não estejam em conformidade com a legislação atual. As denúncias podem ser realizadas ao Canal de denúncias disponibilizado pela empresa nos canais de comunicação internos e no website, ou pelo **SETOR DE INFORMÁTICA**, por telefone, website, ou e-mail, e de forma anônima.

O **ALTA DIREÇÃO** compromete-se a apurar os relatos recebidos com independência, cautela e responsabilidade, de maneira justa e imparcial, utilizando todos os meios disponíveis, a fim de tomar medidas disciplinares e/ou legais cabíveis ao caso, quando necessário. É de responsabilidade de todos o conhecimento, cumprimento e a disseminação desta política. Qualquer violação às diretrizes aqui contidas resultará em medidas disciplinares como: advertências, suspensões, ou ainda a rescisão do contrato de trabalho, de prestação de serviços ou similar.