ÍNDICE

MENSAGEM DA HABITASEC AOS COLABORADORES:

Esta Política de Segurança da Informação da HABITASEC tem o objetivo de detalhar as práticas e o tratamento adequado às informações produzidas na empresa e acordar com todos os colaboradores os seguintes compromissos:

- Nossos colaboradores mantêm reserva sobre os negócios da empresa, guardando sigilo sobre qualquer informação ainda não divulgada para o conhecimento do mercado, bem como sobre a informação de terceiros e clientes obtidos no exercício de suas funções;

- Nossos colaboradores não utilizam estas informações para obter, pessoalmente ou para terceiros, vantagens sobre qualquer natureza.

- A informação é um ativo essencial dos Processos de Negócios da HABITASEC. Informações reservadas ou confidenciais somente são divulgadas com autorização da Diretoria. Todo colaborador que possui acesso a estas informações tem o cuidado de não expô-las a terceiros.

O envolvimento e a adesão consciente de cada um dos colaboradores a essa Política serão fundamentais para consolidarmos o comportamento coletivo cada vez mais atento e seguro quanto ao tratamento das informações internas.

Este documento apresenta as Normas Gerais para uso adequado das informações e recursos de tecnologia na HABITASEC e orientará nossas atitudes sobre o tema, oferecendo padrões de comportamento a serem seguidos.

Atenciosamente,

A DIRETORIA DA HABITASEC

1. CONTROLE DE VERSÃO

Versão 001 – versão inicial do documento	19/10/2017 – Marcos Valle
Versão 002 - versão atualizada	01/03/2022 – Daniela Rodrigues
Versão 003 – versão atualizada	16/02/2024 – Heitor Varela

2. OBJETIVO:

- ✓ O objetivo desta norma é definir as regras para o uso adequado das informações e dos recursos de tecnologia da informação da HABITASEC.

3. APLICA-SE:

- ✓ Todas as Unidades de negócios da empresa.

4. RESPONSABILIDADES:

4.1. Área de Infra-estrutura:

- ✓ Manter atualizada a Política de Segurança da Informação;
- ✓ Elaborar, manter atualizado e testar periodicamente um Plano de Contingência;
- ✓ Tratar dúvidas e questões não contempladas pela Política de Segurança da Informação.

4.2. Diretoria Administrativo-Financeira:

- ✓ Avaliar e deliberar sobre a viabilidade econômico-financeira de projetos apresentados pelo Departamento de TI da HABITASEC e aprovar alterações na política.

4.3. Gestores das áreas:

- ✓ Garantir a aplicação adequada da Política de Segurança da Informação, apoiados pelo Departamento de TI e Diretoria.

4.4. Colaboradores e demais envolvidos

- ✓ Zelar pela utilização adequada das informações, e dos recursos computacionais oferecidos, em conformidade com os objetivos do negócio, missão, visão, valores e com a política de TI.

5. CRITÉRIOS E REGRAS:

5.1. Propriedade e Proteção da Informação:

- ✓ Toda a informação produzida na HABITASEC, ou por ela adquirida, é considerada de sua propriedade, sendo parte do seu patrimônio, não importando a forma de apresentação ou armazenamento. Esta informação deve ser adequadamente protegida;

- ✓ A informação pertence à empresa e só pode ser utilizada no seu interesse. Seu uso ou divulgação externa somente poderá ocorrer quando expressamente autorizado pela organização;
- ✓ As informações devem ser utilizadas exclusivamente para fins relacionados diretamente ao negócio da organização, observando as orientações contidas na Política de Segurança da Informação da HABITASEC;
- ✓ A HABITASEC poderá monitorar o recebimento, envio e conteúdo de todos os emails e documentos de sua propriedade sem prévia notificação aos usuários.

5.2. Divulgação

- ✓ A HABITASEC disponibilizará esta Política de Segurança da Informação no Portal Documentos internos da HABITASEC para acesso de todos os seus colaboradores.

5.3. Contratos de Serviços (Terceiros)

- ✓ Deve ser prevista nos contratos de prestação de serviços, cláusula específica expondo a obrigatoriedade do cumprimento da Política de Segurança da Informação pelo fornecedor contratado pela HABITASEC.

6. CLASSIFICAÇÃO DA INFORMAÇÃO:

- ✓ Informações estratégicas da HABITASEC, enquanto não divulgadas de forma oficial, são consideradas estritamente confidenciais;
- ✓ O Colaborador HABITASEC é responsável por garantir a segurança da informação sob a sua guarda.
- ✓ Não é permitido divulgar informações Confidenciais, seja através de conversas informais, e-mails ou qualquer outro meio de comunicação, sem a prévia autorização.

7. SEGURANÇA FÍSICA E DO AMBIENTE:

7.1. Acesso Físico

- ✓ O acesso físico ao ambiente de TI somente será permitido com o acompanhamento de um colaborador do departamento.
- ✓ O acesso às dependências da HABITASEC em horários alternativos exceto Diretoria, Gerência e Coordenadores deverá ser previamente informado ao Departamento de TI pelo Gestor da área;
- ✓ Para acesso às dependências em horários alternativos (Finais de semana, Feriado etc.) será necessário que o Gestor da área, informe o Departamento de TI com antecedência mínima de 2 dias.

7.2. Zelo com as informações

- ✓ Não devem ser deixadas sobre a mesa de trabalho informações classificadas como confidenciais e/ou estratégicas, salvo em salas com chave, dentro de gavetas ou armários.
- ✓ Quando impresso algum documento, deve-se o quanto antes buscá-lo na impressora (e casos de impressoras compartilhadas);
- ✓ O colaborador deve sempre bloquear sua estação de trabalho quando interromper o uso, mesmo que por breves momentos;

- ✓ As informações Confidenciais devem ser totalmente destruídas quando não mais necessárias, independentemente do tipo de mídia em que estiverem armazenadas (Disquete, Pen Drive, CD, DVD, etc.);
- ✓ Arquivos de dados relevantes nunca devem ser armazenados no disco local do computador, devendo ser utilizados os *drives* da rede para tal, onde dispositivos de segurança asseguram o correto tratamento desta informação.

7.3. Computação Móvel

- ✓ O acesso a computação móvel será permitido somente para Diretoria, exceções devem ser autorizadas pelo Diretor Administrativo e pelo Gerente de TI.
- ✓ Quando solicitado algum equipamento, o usuário preencherá um termo de responsabilidade disponibilizado pelo Departamento de TI. O usuário irá zelar pelo equipamento sob sua guarda, devendo utilizá-lo e movimentá-lo atendendo exclusivamente aos interesses da HABITASEC.
- ✓ Não é permitido o uso de equipamentos pessoais, sistemas ou arquivos nas dependências da empresa ou no desenvolvimento das funções do colaborador.

8. OPERAÇÃO DO AMBIENTE COMPUTACIONAL:

8.1. Operação dos Recursos de Processamento das Informações

- **Conexões de Rede**
  - ✓ Só é permitida a conexão de fornecedores na rede dentro da HABITASEC pela rede Wireless, desde que sejam garantidos os requisitos mínimos de segurança, definidos nessa Política de Segurança da Informação da HABITASEC. Equipamentos conectados à rede Wireless devem ter antivírus com a data da última atualização não superior a três dias;

- ✓ A HABITASEC poderá auditar os equipamentos dos colaboradores para garantir a segurança geral de seu ambiente computacional sem prévio aviso;
- ✓ E proibido utilizar conexão discada via modem, ADSL ou quaisquer outras formas, nos equipamentos que estejam, ao mesmo tempo, conectados na rede local da HABITASEC.

- **Senhas**
  - ✓ A senha é pessoal e intransferível, devendo obedecer aos padrões divulgados pela empresa. O colaborador é responsável por todas as transações realizadas nos sistemas disponibilizados;
  - ✓ A senha não deve, sob hipótese alguma, ser compartilhada com outras pessoas;
  - ✓ O usuário não deve armazenar sua senha em arquivos de computador e tampouco escrevê-la em papéis ou outro tipo de mídia;
  - ✓ As senhas de Logon na rede (WINDOWS) devem estar de acordo com os seguintes aspectos:
    a) Conter no mínimo 6 (seis) caracteres;
    b) Possuir validade de no máximo 42 dias;
    c) Possuir Letras e Números;
    d) Devem ser criptografadas quando transmitidas ou armazenadas;
  - ✓ As senhas do Protheus 10 devem estar de acordo com os seguintes aspectos:
    e) Conter no mínimo 6 (quatro) caracteres;
    f) Possuir validade de no máximo 42 dias;
    g) Devem ser criptografadas quando transmitidas ou armazenadas;
  - ✓ Critérios de senhas de outros sistemas de trabalho dos departamentos devem ser decididos pelos Gestores da área.

- **Hardware e Software**
  - ✓ Não é permitida a instalação e Utilização de unidades de armazenamentos removíveis (pen drives, HDs externos, cartão de memória, mp3 e outros) salvo (Diretoria e Gerencia).
  - ✓ Não é permitido compra de equipamentos de Tecnologia e Softwares sem a prévia comunicação e aprovação de TI.

- **Alterações de Configuração**
  - ✓ As configurações de hardware e software dos computadores disponibilizados pela HABITASEC não devem ser alteradas. Caso haja necessidade de algum tipo de alteração, o Departamento de TI deverá ser acionado através de solicitação por email.
- **Internet**
  - ✓ A Internet é uma ferramenta de trabalho utilizada pelos colaboradores como apoio ao desenvolvimento de suas atividades e competências;
  - ✓ A autorização de acesso à Internet deve ser solicitada pelo Gestor do colaborador;
  - ✓ Não é permitido o acesso a emails pessoais e software de comunicação entre outros, caso necessário devera ser solicitada autorização pelo gestor responsável e aprovado pelo Gerente de Ti e Diretor Responsável.
  - ✓ Utilização de SITES somente relacionada à atividade do colaborador e aprovado pelo Gerente de Ti e Diretor Responsável.

8.2. Proteção contra Software Malicioso

- ✓ O software de proteção contra vírus deve ser instalado, ativado e atualizado diariamente em todos os computadores ligados à rede de dados da HABITASEC.

8.3. Cópia de Segurança (backup)

- ✓ Cabe ao Departamento de TI realizar regularmente a cópia dos dados e informações mantidas nos equipamentos de armazenamento nos servidores da empresa;
- ✓ Backup de emails armazenados no computador local de usuários não será realizado, exceto diretoria e gerência que utilizam computadores móveis, ao qual serão armazenados uma vez por semana.
- ✓ Arquivos de conteúdo considerado impróprio para o negocio não devem ser armazenados nos computadores da HABITASEC;
- ✓ Os *drives* internos (discos C, E, pen drives, etc.) não devem ser utilizados para armazenar dados relevantes para a HABITASEC. O backup dos arquivos armazenados nestes locais é de responsabilidade do próprio usuário;

8.4. Tratamento de Mídia

- ✓ Não é permitido realizar cópia ou divulgar informações Confidenciais para uso pessoal ou de terceiros. Tais cópias ou divulgações, quando necessárias, devem ser autorizadas pelo respectivo Gestor;

8.5. Troca de Informações

- **Uso do Correio Eletrônico (e-mail)**
  - ✓ A autorização de acesso ao correio eletrônico deve ser solicitada ao Departamento de TI pelo DAP (RH Administrativo);
  - ✓ O Correio Eletrônico é uma ferramenta de trabalho utilizada pelos usuários como apoio ao desenvolvimento de suas atividades profissionais;
  - ✓ Não é permitido utilizar o Correio Eletrônico para o envio de mensagens ou arquivos de conteúdo considerado impróprio pela empresa;
  - ✓ É considerado impróprio o conteúdo que não está em conformidade com as regras legais, a moral, a integridade e os bons costumes, tais como campanhas políticas, religiosas,

venda de produtos, boatos, jogos, músicas, filmes, vídeos e fotos que não esteja na conformidade do negocio.

- ✓ O endereço oficial da empresa (@HABITASEC.com.br), assim como as Caixas Postais a eles associadas são de propriedade da HABITASEC;
- ✓ É proibido o download e envio de arquivos anexados ao e-mail com as extensões *.exe, *.pif, *.bat, *.com, *.scr, *.mp3, *.wav, *.wma, *.vbs, *.reg;
- ✓ Todos os emails do domínio, exceto os de gerentes e diretores, serão armazenados pelo setor de TI, para auditorias internas e externas, e poderão ser consultados com a autorização da diretoria a qualquer momento sem prévio aviso.
- ✓ Práticas recomendadas na utilização o e-mail:
  a) Envie e-mails apenas para os destinatários que realmente precisam da informação;
  b) Seja breve, pois assim, dificilmente as pessoas deixarão de ler a sua mensagem;
  c) Sempre que possível, não utilize anexos no e-mail;
  d) Seja educado, não escreva nada que não diria pessoalmente.

- **Uso de Criptografia**
  - ✓ Somente é permitida a utilização de mecanismos de criptografia homologados pela HABITASEC. Em caso de necessidades adicionais, o Departamento de TI deverá ser acionada através de email admin.ti@HABITASEC.com.br.

8.6. Softwares e Recursos de Informática

- **Instalação de Softwares**
  - ✓ Somente é permitida a utilização de software devidamente homologado, licenciado, instalado e controlado pelo Departamento de TI. Qualquer necessidade adicional deverá ser

solicitada através de abertura de chamado pelo e-mail admin.ti@HABITASEC.com.br.

- **Instalação e movimentação de Recursos de Informática**
  - ✓ A instalação, controle, movimentação e manutenção de recursos computacionais de propriedade da HABITASEC são de responsabilidade exclusiva do Departamento de TI.

9. CONTROLE DE ACESSO:

9.1. Acesso Lógico

- ✓ Cada usuário de recursos computacionais da HABITASEC deve possuir uma identificação (ID), a qual será utilizada como "conta de acesso" aos sistemas e redes da empresa determinadas a sua área;
- ✓ O cadastramento do usuário para o acesso aos recursos computacionais deve ser solicitado pelo RH Administrativo e gestor da área ao Departamento de TI, a qual estabelecerá os perfis e autorizações de acesso pelo modelo de documento Cadastro de Usuário;
- ✓ O usuário deve ter acesso somente às informações e recursos que forem necessários para a realização de suas atividades;
- ✓ Todo sistema aplicativo deve possuir controle de acesso de modo a assegurar o uso apenas por usuário autorizado;
- ✓ As movimentações de pessoal (admissões, transferências, promoções, demissões, etc.) devem ser comunicadas pelo RH Administrativo ao Departamento de TI, a fim de que as devidas atualizações nos ambientes computacionais sejam realizadas;
- ✓ Cabe ao Gestor responsável por contratos de fornecedores, quando do encerramento dos mesmos, solicitar ao Departamento de TI, via abertura de chamados pelo Email @HABITASEC.com.br , o cancelamento dos acessos concedidos previamente.

9.2. Desligamentos

- ✓ Será de responsabilidade do RH administrativo informar os desligamentos de colaboradores imediatamente para o Departamento de TI, ao qual realizará os bloqueios de acesso de imediato;
- ✓ O colaborador deverá entregar todos os equipamentos de sua responsabilidade para o setor de TI no momento de seu desligamento Como: CELULARES, NOTEBOOKS, PEN DRIVES E OUTROS, sobe pena de restituição de valores.
- ✓ Dados de usuários desligados da HABITASEC serão armazenados durante Três meses para utilização exclusiva da HABITASEC e o email redirecionado para o gestor da área no período de um mês. O colaborador desligado não poderá realizar cópia de arquivos para sua utilização fora da empresa.

10. PLANO DE CONTINGÊNCIA:

- ✓ Cabe ao Departamento de TI elaborar, manter atualizado e testar periodicamente um Plano de Contingência – Ambiente de Desenvolvimento que garanta a continuidade das atividades críticas aos negócios da HABITASEC.

11. CONFORMIDADE:

- ✓ A HABITASEC, seus colaboradores e todos aqueles que estejam envolvidos com suas atividades devem estar em conformidade com essa Política de Segurança da Informação.

12. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:

Violações a essa Política estão sujeitas a sansões disciplinares, observadas a natureza e gravidade da infração.

Ao identificar ou suspeitar de possível violação das Diretrizes estabelecidas nessa Política o colaborador deve buscar orientação nas seguintes instâncias: Gestor imediato, área de RH, Diretoria Administrativa ou Gerencia de TI .

Em caso de dúvida sobre essa Política de Segurança da Informação entre em contato com ao Departamento de TI: @HABITASEC.com.br.