1. OBJETIVO

Definir as diretrizes de Segurança da Informação e privacidade da Hands4IT.

2. ABRANGÊNCIA

Todas as unidades de negócios, colaboradores, prestadores de serviços, parceiros e fornecedores da Hands4IT.

3. RESPONSÁVEL

A alta direção da Hands4IT é responsável pela viabilização das condições necessárias para a devida aplicabilidade desta Política e a Diretoria de Operações é responsável pela atualização dessa Política e Normas.

4. DIVULGAÇÃO E DECLARAÇÃO DE RESPONSABILIDADE

A Política deve ser de conhecimento de todos. Sua divulgação e educação são de suma importância para a empresa, e poderá ser divulgada e publicada de forma digital.

Cabe as unidades de negócios juntamente com a equipe de Diretoria de Operações e equipe de marketing e divulgação analisar e definir a melhor forma de divulgação, considerando e respeitando a cultura e costumes, leis e regulamentos vigentes e evitando qualquer tipo de discriminação.

Todos os colaboradores, prestadores de serviços, parceiros e fornecedores que tenha acesso a informações, comprometendo-se a respeitar esta Política e suas normas de forma integral.

5. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para organização ou seus clientes. Ela pode estar guardada para uso restrito ou exposta ao cliente para consulta ou manuseio.

Entende-se por privacidade o direito da inviolabilidade à intimidade, à vida privada, à honra e a imagem das pessoas.

Todo tipo de ativo de informação é classificado, podendo ser rotulado como: Confidencial, Privado, Sensível ou Público. Independente da forma apresentada ou o meio do qual a informação é compartilhada ou armazenada, a informação é o maior ativo da Hands4IT e de seus clientes, e por

isso essencial ao negócio, por esses motivos deverá ser devidamente protegida e utilizada de modo ético e seguro.

Para tanto a Política de Segurança da Informação definiu os pilares de:

a) Confidencialidade: Garantir que a informação não seja revelada ou esteja disponível para indivíduos, entidades e processos não autorizados;

b) Integridade: Garantir a salvaguarda da exatidão e totalidade da informação e dos métodos de processamento.

c) Disponibilidade: Garantir que a informação esteja sempre acessível e disponível quando necessário.

Considerando a:

1. Prontidão: Ser acessível sempre que necessária,

2. Continuidade: Manter-se disponível mesmo quando houver falhas nos sistemas,

3. Robustez: Atender a todos os usuários do sistema sem que haja uma degradação que comprometa o resultado.

d) Autenticidade: Garantir que a autoria seja confirmada.

6. DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO

Para endereçar todo o esforço e manutenção necessária para a Segurança da Informação, estabelece as seguintes diretrizes:

a) Uma estrutura de Segurança da Informação e Privacidade foi estabelecida e mantida com apoio da alta direção, através de um Sistema de Gestão de Segurança da Informação e Privacidade.

b) A informação deverá ser utilizada com senso de responsabilidade e de modo ético e seguro por todos, em benefício exclusivo dos negócios corporativos;

c) A Hands4IT reserva-se o direito de monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Para tanto foram criados e implantados controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgou necessário para reduzir os riscos;

d) Todos os ativos de informação estão devidamente identificados, classificados e monitorados;

e) A identificação de cada usuário da Hands4IT é única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;

f) Todos os riscos deverão ser analisados, classificados e apresentados à Diretoria de Operações, que deliberará sobre o Tratamento adequado para tais;

g) Todos os incidentes de segurança devem ser reportados, para que sejam analisados, avaliados e tratados pela área responsável.

h) A Hands4IT, através de sua direção, identifica, aprimora, documenta e mantém atualizadas as leis que regulamentam suas atividades, bem como dos aspectos de propriedade intelectual.

i) A Hands4IT, através de sua direção definiu os Objetivos Estratégicos da Segurança da Informação, considerando esta Política, os requisitos da Segurança da Informação, bem como sua aplicabilidade e os resultados da Gestão de Riscos.

7. GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Para manter um nível satisfatório de segurança, elegeu-se que a Diretoria de Operações adotará as seguintes normas, e outras que possam ser criadas, para sustentar as diretrizes apresentadas:

a) Norma de Controle de Acesso: O controle de acesso dos colaboradores internos ou externos aos ativos de informação deve ser devidamente aprovado pelo responsável da informação (gestor, diretoria ou responsável), a qual o acesso permitirá a manipulação, quer seja para simples consulta ou para alteração;

b) Norma de Correio Eletrônico: O uso do e-mail sob @hands4it.com*, será permitido para colaboradores internos e externos, e para terceiros somente quando for necessário, e por tempo determinado pela gerência da área solicitante mediante a Termo de responsabilidade. Este tempo poderá ser prorrogado mediante nova solicitação da gerência da área.

c) Norma de Cópias de Diretoria de Operações (Backup): Cópias de segurança (backup) através de mídias específicas de informações que são consideradas vitais para o sistema e para a retomada das atividades da área em caso de contingência;

d) Norma de Classificação e Manuseio da Informação: As informações devem ser classificadas e manuseadas de acordo com a confidencialidade e as proteções necessárias, da seguinte forma: Pública, Sensível, Privada e Confidencial, e devem ser tratadas, armazenadas e descartadas de maneira correta para garantir os aspectos Segurança da Informação e privacidade do negócio da Hands4IT e de seus clientes;

e) Norma de Conduta Ética de Colaboradores: As responsabilidades de todos quanto a Segurança da Informação, seguindo requisitos mínimos de conduta e ética estão definidas;

f) Norma de Gestão de Ativos: Os ativos tangíveis e intangíveis de informação estão identificados de forma individual, inventariados, protegidos e monitorados de acessos indevidos. As mídias são gerenciadas de forma adequada, conforme os requisitos de Segurança da Informação. O acesso remoto deve estar registrado e o seu tempo definido.

g) Norma de Gerenciamento de Chaves Criptográficas e Transmissão de Informações: Um conjunto de regras para garantir a padronização das técnicas criptográficas, a aplicação adequada das mesmas e responsabilidades para manter a segurança no transporte ou armazenamento das informações independente do meio utilizado. Quanto à transmissão de informações, este recurso é utilizado para garantir a privacidade na comunicação dos dados da Hands4IT e de seus clientes;

h) Norma de Gerenciamento de Mudanças: Um processo de gestão de mudanças está em vigor para garantir que controles e modificações nos sistemas ou recursos de processamento da informação sejam realizados com planejamento, visando não ocasionar falhas operacionais ou de segurança no ambiente produtivo da organização;

i) Norma de Análise, Avaliação e Tratamento de Riscos: Os riscos são identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade);

j) Norma de Gestão de Incidentes de Segurança da Informação: Todo o incidente deve ser reportado a área de Diretoria de Operações através do canal sdk@hands4it.com que analisará o incidente e tomará as ações devidas, repassando a tratativa as áreas responsáveis;

k) Norma de Tecnologia da Informação e Uso aceitável de Ativos: Estão regulamentadas as responsabilidades de Tecnologia da Informação e restrições do uso de ativos na organização;

l) Norma de Indicadores e Métricas da Segurança da Informação: Para garantir a melhoria contínua, com base na norma ISO/IEC 27001:2013, todos os indicadores e métricas devem ser monitorados para aplicação do ciclo PDCA;

m) Norma de Conformidade: Define regras para garantir que não ocorram violações jurídicas, regulamentares ou contratuais nos requisitos de Segurança da Informação na organização;

n) Norma de Segurança Física e Ambiente: Garantir que o acesso físico às instalações onde os ativos de TI e informações críticas à continuidade do negócio estejam armazenados sejam controlados de forma a garantir a sua proteção, disponibilidade, integridade e confidencialidade.

o) Norma de fiscalizações. Certificar que é uma autoridade competente e identificá-la. Certificar de que é uma fiscalização com o escopo verdadeiro. Certificar de que o caso não tenha se tornado público. Encaminhamento ao jurídico para análise e resposta legal, bem como à Diretoria de Operações.

p) Norma de Fornecedores: Garantir que os contratos com fornecedores, parceiros e terceiros, estejam sempre pautados em uma postura ética compatível com os princípios, valores da Hands4IT e promovam uma relação mais justa e sustentável.

Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação dos requisitos previstos nesta política o responsável e/ou solicitante deverá documentá-las imediatamente à área de Diretoria de Operações ou área responsável para que possibilite a adoção de medidas alternativas que minimizem os riscos, bem como um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

8. MONITORAMENTO E AUDITORIA

A Hands4IT monitora e registra todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Para anto a organização mantém controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgou necessário para reduzir os riscos, e reservar-se o direito de:

a) Implantar outros sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônicos, navegação, Internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;

b) Inspecionar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente, visando assegurar o rígido cumprimento desta política.

c) Instalar outros sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso.

9. PENALIDADES

Para toda e qualquer infração à Segurança da Informação e suas normas, a Diretoria de Operações deverá abrir um incidente, tratando de acordo com a Norma de Gestão de Incidentes, e por conseguinte, apurada através de procedimentos internos, que deve ser conduzido pelo gestor da área em que se encontra alocado o profissional que cometeu a infração, em conjunto com a área de Recursos Humanos

Caso a Diretoria de Operações julgue cabível, o colaborador envolvido poderá, enquanto durar o processo de apuração interna, ser afastado da função ou suspenso.

Ao colaborador suspeito de cometer violações à Política e Normas de Segurança da Informação, deverá ser assegurado tratamento justo e correto, sendo que toda e qualquer medida resultante de sua infração deverá ser aplicada com proporcionalidade à ocorrência com base no Código de Conduta, Termo de Confidencialidade, Manual do Colaborador e Processo Disciplinar Hands4IT e legislações vigentes.

A Hands4IT exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, terceiros e parceiros, reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais cabíveis.

10. DECLARAÇÃO DE ESCOPO

A Hands4IT está comprometida em promover uma gestão sistemática de Segurança da Informação que garanta a proteção de seus processos, ativos de informação, e informações de seus clientes. Para atingir este objetivo, a Hands4IT implementou um Sistema de Gestão de Segurança da Informação em conformidade com a norma ISO/IEC 27001

Revisão: maio/2022.