1. OBJETIVO

Definir as diretrizes e procedimentos para garantir a segurança das informações da POIESIS e de terceiros, assim como a correta utilização dos sistemas de informação e comunicação utilizados dentro do ambiente da POIESIS.

2. APLICABILIDADE

Esta política se aplica a todas as áreas e a todos os colaboradores da Organização, bem como terceiros contratados que, no exercício da atividade contratada, tenham acesso às informações da POIESIS, bem como rede e/ou sistemas corporativos de informação e comunicação da POIESIS.

3. ATRIBUIÇÕES E RESPONSABILIDADES

São definidas a seguir as atribuições e responsabilidades específicas, segundo as competências de cada grau funcional dentro da Organização, cabendo a cada um, o cumprimento das diretrizes desta política na sua íntegra:

3.1. Diretor Executivo e Diretor Administrativo Financeiro

- Aprovar a Política de Segurança da Informação
- Aprovar tratamento dos casos de não conformidade avaliados pelo Comitê de Integridade

3.2. Comitê de Integridade

- Avaliar a Política de Segurança da Informação, assim como eventuais atualizações demandadas
- Tratar todas as ocorrências identificadas relacionadas à não conformidade para com as diretrizes desta política, nos casos classificados como desvio de conduta.

3.3. Gestores de Unidades e Áreas

- Cumprir e fazer cumprir as diretrizes desta política em suas respectivas áreas;
- Propor mudanças nesta política de acordo com as necessidades identificadas na sua área de atuação.

3.4. Área de Tecnologia e Integridade

- Definir e executar os procedimentos para tratamento de incidentes de segurança da informação;
- Reportar imediatamente para a Diretoria competente os incidentes que coloquem em risco a operação da Organização;
- Propor atualizações à política em concordância com a evolução e atualização da Organização;

3.5. Todos os colaboradores da Organização

- Cumprir as regras definidas nesta política;
- Reportar de imediato ao gestor da área, ou ao supervisor de TI, qualquer incidente de segurança ou, até mesmo, riscos identificados;

3.6. Terceiros contratados pela POIESIS que tenham acesso às informações da POIESIS, bem como rede e/ou sistemas corporativos de informação e comunicação da POIESIS.

- Cumprir às determinações desta política durante o exercício da atividade contratada;
- Reportar imediatamente para o gestor da POIESIS que é responsável pelo contrato os incidentes de segurança da informação que forem identificados. Este deverá reportar o incidente, de imediato, ao supervisor de TI.

4. REGRAS E PROCEDIMENTOS

4.1. Uso correto e seguro da Informação

- Toda informação ou conhecimento gerado pelas atividades desenvolvidas pela POIESIS deve ser tratada com cuidado e responsabilidade, principalmente nos casos de divulgação ou transferência/repasse a terceiros, os quais devem ser previamente aprovados pelos gestores responsáveis.
- Casos de divulgação em redes sociais, fóruns e blogs, devem sempre ser analisados e acompanhados pela área de Comunicação.
- No caso de informação definida como confidencial, é expressamente proibida qualquer tipo de divulgação ou transferência a terceiros, salvo quando previamente analisada e aprovada pelas áreas e gestores competentes.

4.2. Privacidade sobre Dados Pessoais

- Todo tratamento de Dados Pessoais realizado pela POIESIS ou por seus contratados devem atuar de acordo com as disposições da LGPD (Lei Geral de Proteção de Dados).
- Dados pessoais são considerados confidenciais e como tal devem ser tratados com a máxima privacidade, seguindo as diretrizes da política interna específica de Proteção de Dados Pessoais.

4.3. Uso correto e profissional do e-mail corporativo

- O e-mail corporativo deve ser utilizado exclusivamente para os propósitos das atividades da Organização, e não deve ser utilizada para comunicação de assuntos pessoais;
- E-mails recebidos de contatos anônimos, principalmente se contiverem links ou anexos, não devem ser acessados e devem ser descartados. Na dúvida, entrar em contato com o equipe de TI para que possam ser analisados e tratados de forma correta;
- É expressamente proibida a utilização de e-mail para qualquer conteúdo relacionado à pornografia, pedofilia, discriminação racial ou social, incitação à violência ou desordem, assédio moral ou sexual, ou outros atributos definidos por lei, bem como para envio de "*spam*", independentemente do assunto abordado. Entende-se como "*spam*" o envio indiscriminado de e-mails para várias pessoas simultaneamente.

4.4. Uso correto e profissional da Internet corporativa

- O acesso corporativo de Internet deve ser utilizado somente para os propósitos das atividades da Organização;
- É proibido utilizar o acesso corporativo de Internet para conteúdos relacionados à pornografia, pedofilia, discriminação racial ou social, incitação à violência ou desordem, assédio moral ou sexual, ou outros atributos definidos por lei, bem como para o acesso ilegal aos sites.

4.5. Segurança para as Senhas de Acesso aos Sistemas da Organização

- A senha de acesso à rede corporativa ou aos sistemas de informação e gestão, são de uso pessoal e intransferível. Sendo assim, a responsabilidade pela sua definição, guarda e utilização é do próprio usuário, que deve sempre seguir as orientações e diretrizes fornecidas pelo supervisor de TI;
- Para a segurança das suas senhas pessoais, evite a utilização de datas de aniversário, nomes, números de documentos ou outras formas fáceis de serem tentados por pessoas que queiram utilizar-se do seu acesso aos sistemas da Organização, mudando-as frequentemente (pelo menos a cada três meses) e evitando deixá-las anotadas em locais de fácil acesso.

4.6. Uso correto e profissional dos computadores corporativos

- Para as atividades na Organização, utilize apenas computadores disponibilizados pela equipe de TI, pois estes já terão instalados os programas de segurança e de produtividades necessários para a execução das suas atividades na Organização;
- O computador corporativo deve sempre ser utilizado com responsabilidade, zelando pelo equipamento e também pelas informações da POIESIS nele contido, tanto dentro do ambiente da POIESIS quanto em ambiente externo, mantendo-o constantemente sob a sua guarda;
- Ao descartar um computador da Organização, o mesmo deve ser enviado ou recolhido pela equipe de TI, que deverá, além de outros procedimentos, realizar um backup dos dados (caso necessário) e depois apagar os dados do disco rígido, para garantir que informações da Organização e de terceiros não sejam acessados por pessoas não autorizadas.

4.7. Uso correto e profissional do software

- Todo e qualquer software (programa, aplicativo) deve ser obrigatoriamente analisado e aprovado pelo supervisor de TI antes da sua instalação nos computadores corporativos.
- A utilização e controle dos “sistemas”, de gestão administrativa ou operacional, deve seguir a instrução técnica específica da área de Tecnologia e Integridade.
- A controle dos perfis de acesso dos sistemas de gestão utilizados na POIESIS são de responsabilidade do gestor responsável por cada sistema de gestão, que deverá manter uma relação atualizada de todos os usuários ativos do respectivo sistema.

4.8. Uso seguro e profissional da rede corporativa

- Não é permitido conectar qualquer dispositivo na rede corporativa da Organização, com exceção dos previamente analisados e formalmente aprovados pelo supervisor de TI;
- O acesso à rede corporativa da Organização é permitido apenas aos funcionários, e terceiros a serviço da Organização, cujas atividades demandam este tipo de acesso, restrito apenas às funcionalidades, pastas e diretórios necessários para a execução das respectivas atividades;
- A requisição de acesso a qualquer pasta da rede corporativa deve ser feita ao supervisor de TI, que deverá requisitar uma autorização formal por parte do respectivo responsável das pastas envolvidas na requisição de acesso.

4.9. Uso correto de celular corporativo

- Qualquer celular fornecido pela Organização deverá ser utilizado exclusivamente para a execução das atividades da POIESIS. Os aparelhos serão entregues com plano para ligações e outros serviços, pré-definidos. O usuário deverá tomar os cuidados necessários para manter o

bom funcionamento do equipamento, assim como a utilização correta da linha alocada no chip do respectivo aparelho fornecido.

- O usuário não deverá, em hipótese alguma, trocar o equipamento, ou qualquer um de seus acessórios, com outro colaborador, sem autorização prévia da equipe de TI.
- Os acessórios que acompanham o aparelho, tais como, carregadores de parede, carregadores veiculares, cabos de conexão, ou outros itens que sejam imprescindíveis, sempre serão fornecidos pela equipe de TI, não sendo permitido o uso de qualquer outro tipo de acessório, exceto quando autorizado pela equipe de TI.
- Procedimentos de configuração, assim como a instalação de aplicativos no aparelho, só deverão ser feitas mediante autorização prévia e orientação da equipe de TI.
- O usuário deverá ter cuidado com as informações captadas e armazenadas pelos aplicativos. É proibida a coleta de quaisquer dados pessoais sem consentimento de seus titulares. O armazenamento de dados pessoais nos celulares corporativos deve ser temporário, e tão logo sejam tratados conforme definição prévia, devem ser deletados do aparelho.

4.10. Atitudes diárias de segurança

- Não deixar acessíveis documentos ou arquivos com dados pessoais, informações confidenciais ou sensíveis;
- Guardar ou travar fisicamente os computadores portáteis;
- Bloquear o acesso ao seu computador ao sair de sua mesa;
- Configurar o seu protetor de tela com senha.

4.11. Comunicação de incidente de segurança da informação

Entende-se como “incidente” de segurança da informação, qualquer fato ou evento que tenha ocorrido ou que venha a ocorrer, que possa colocar em risco a operação da Organização, relacionado direta ou indiretamente à perda, roubo, acesso ou divulgação indevida de informações da Organização.

Deve se comunicar imediatamente ao supervisor de TI, qualquer caso de:

- Ocorrência de vírus no computador, ou em outros dispositivos corporativos;
- Perda ou roubo de computadores corporativos, ou outros dispositivos corporativos;
- Envio acidental de informações sensíveis ou confidenciais;
- Identificação de qualquer quebra das regras definidas nesta política.

O supervisor de TI deve informar ao Diretor de competência, todas as ocorrências que possam colocar em risco a operação da POIESIS, e tomar as devidas contramedidas para minimização dos riscos para a Organização.

Todos os casos de não conformidade identificados devem ser tratados no âmbito do Comitê de Integridade.

4.12. Procedimentos técnicos de gestão do parque tecnológico

Os procedimentos técnicos executados pelo supervisor de TI, sua equipe e pelo prestador de serviço técnico especializado em TI vigente, estão definidos no Manual de TI da POIESIS, e engloba procedimentos como:

- Classificação de nível de confidencialidade de documentos

- Disponibilização de equipamentos de TI para colaboradores e terceiros contratados
- Tratamento de incidentes de TI
- Segurança Lógica e Física
- Registro de Eventos
- Backup
- Disponibilidade

5. CANAL ÚNICO PARA ESCLARECIMENTO DE DÚVIDAS RELACIONADAS À SEGURANÇA DA INFORMAÇÃO

Toda e qualquer dúvida relacionada com a segurança da informação deve ser direcionada e esclarecida junto ao supervisor de TI.

6. PENALIDADES APLICÁVEIS

As violações das regras definidas nesta política serão tratadas pelo Comitê de Integridade e poderão resultar em punições administrativas determinadas no Manual de Recursos Humanos.

No caso de violação das regras definidas nesta política por profissionais das empresas contratadas para prestação de serviços para a POIESIS, a penalidade poderá ser o cancelamento do contrato e/ou ressarcimento do prejuízo financeiro causado pela violação.

7. DISPOSIÇÕES FINAIS

Esta política entra em vigor a partir da sua aprovação, e deverá ser disponibilizada na Intranet.

São Paulo, 01 de outubro de 2021.

DocuSigned by:
Clovis Carvalho
7318CE7D63C64A8...

Clovis Carvalho
Diretor Executivo

DocuSigned by:
467D3138E3584E4...

Plinio Correa
Diretor Administrativo Financeiro