A. Objetivo

A presente Política de Segurança da Informação e Cibernética ("Política") tem por objetivo estabelecer diretrizes para proteger e salvaguardar os ativos de informação; nortear a definição de normas e procedimentos específicos de Segurança da Informação; e, implementar controles e procedimentos para reduzir a vulnerabilidade a incidentes da Companhia.

B. Abrangência

Todos os colaboradores, incluindo terceirizados, estagiários e jovens aprendizes ("colaboradores") da Beephish Treinamento e Capacitação LTDA.

C. Princípios, Regras e Procedimentos

1. Sobre a Segurança da Informação e Cibernética

1.1. A Companhia possui como objetivo desenvolver processos e produtos considerando os pilares e as boas práticas de segurança da informação, apoiada na gestão dos riscos cibernéticos como assunto estratégico ao negócio, e fomentar a cultura de segurança entre todos os colaboradores para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

1.2. A Companhia estabelece os seguintes pilares:

1.2.1. **Confidencialidade**: garantir que a informação somente estará acessível para pessoas autorizadas;

1.2.2. **Integridade**: garantir que a informação, processada, armazenada ou transmitida, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;

1.2.3. **Disponibilidade**: garantir que a informação estará disponível sempre que for necessário.

1.3. Para desenvolvimento dos produtos e processos da Companhia, são considerados os seguintes princípios:

1.3.1. **Autenticidade**: garantir que a informação é proveniente da fonte original e que não foi alvo de alterações;

1.3.2. **Irretratabilidade ou não repúdio**: garantir que o legítimo autor da informação não possa negar sua autoria;

1.3.3. **Conformidade**: garantir que os processos da Companhia estejam de acordo com os regulamentos, normativos e leis vigentes aplicáveis, de forma a seguir rigorosamente todos os protocolos exigidos no seu setor de atuação.

1.4. A Companhia considera que os ativos de informação são todos aqueles gerados ou desenvolvidos para o negócio, como consentimentos de clientes e pessoas ligadas à Companhia (*opt-in* e *opt-out*), dados cadastrais de clientes e colaboradores, além de conversas e gravações com os clientes. Os ativos de informação podem estar presentes em diversas formas, tais como: arquivos digitais, mídias externas, documentos impressos, documentos digitalmente assinados, dispositivos móveis, bancos de dados e gravações de áudio.

1.5. Os ativos de informação, independentemente da forma apresentada, compartilhada ou armazenada, devem ser utilizados apenas para a sua finalidade devidamente autorizada, sendo sujeitos a monitoramento e auditoria.

1.6. Um responsável deve ser atribuído para todo ativo de informação, que deverá ser devidamente classificado quanto ao seu nível de confidencialidade, de acordo com os critérios estabelecidos em norma específica, e adequadamente protegido de quaisquer riscos, bem como de ameaças que possam comprometer o negócio da Companhia.

2. Diretrizes Gerais de Segurança da Informação e Cibernética

2.1. A Companhia possui como diretrizes gerais:

2.1.1. Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificação, destruição ou divulgação não autorizada;

2.1.2. Realizar a adequada classificação das informações e garantir a continuidade do processamento, conforme os critérios e princípios indicados nos normativos internos;

2.1.3. Garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;

2.1.4. Zelar pela integridade da sua infraestrutura tecnológica na qual são armazenados, processados ou, de qualquer outra forma, tratados os dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a dados internos e confidenciais.

2.1.5. Garantir que as intervenções realizadas no ambiente tecnológico, como auditorias, testes de segurança ou outras atividades no ambiente que possam, de alguma forma, impactar os sistemas operacionais ou os processos de negócio, sejam previamente acordadas entre o solicitante e o responsável pelo ambiente.

2.1.6. Atender às leis e normas que regulamentam as suas atividades.

2.2. Em vistas ao cumprimento das diretrizes acima elencadas, a Companhia:

2.2.1. Adota procedimentos e controles de segurança para atender aos objetivos de segurança cibernética, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra *softwares* maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso, segregação de funções, segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, conforme normativos internos.

2.2.2. Controla, monitora, restringe o acesso aos ativos de informação a menor permissão e privilégios possíveis, conforme descrito em norma interna.

2.2.3. Aplica os procedimentos e controles citados anteriormente, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas em suas atividades.

2.2.4. Possui controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis.

2.2.5. Realiza ações para prevenir, identificar, registrar e responder incidentes e crises de segurança que envolvam o seu ambiente tecnológico e que possam ocasionar o comprometimento de seus pilares de segurança da informação ou gerar impacto de imagem, financeiros ou operacionais.

2.2.6. Classifica os incidentes de segurança da informação e cibernética conforme sua relevância e de acordo com (i) a classificação das informações envolvidas; e (ii) o impacto na continuidade dos negócios da Companhia, conforme descritos em normas internas específicas.

2.2.7. Realiza o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Companhia, que abrangem, inclusive, informações recebidas de empresas prestadoras de serviços a terceiros.

2.2.14. Estabelece regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância, conforme normativo interno. Toda informação possui um proprietário, é classificada e recebe os devidos controles, que garantem sua confidencialidade, condizendo com as boas práticas de mercado e regulamentações vigentes.

2.2.15. Adota mecanismos para disseminação da cultura de segurança da informação e cibernética na Companhia, incluindo:

2.2.15.1. A implementação de programa de treinamento anual para colaboradores;

2.2.15.2. A implementação de programa de avaliação periódica de colaboradores para apuração do nível de conhecimento quanto ao tema segurança da informação e cibernética;

2.2.15.3. A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; e

2.2.15.4. O comprometimento da administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

D. Gestão de Consequências

O não cumprimento das diretrizes desta Política enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem, conforme a respectiva gravidade do descumprimento e de acordo com normativos internos, sendo aplicáveis a todas as pessoas descritas no item "Abrangência" desta Política.

E. Responsabilidades

- **Administradores, Colaboradores e Prestadores de Serviço:** Observar e zelar pelo cumprimento da presente Política. Atuar de forma ética e responsável quando tomar conhecimento de incidentes, compartilhando informações com os responsáveis pelo seu tratamento e tomando todas as ações cabíveis para minimizar os potenciais danos, de acordo com o procedimento Plano de Resposta a Incidentes. Compreender e desempenhar o papel da segurança da informação em suas atividades diárias.

F. Documentação Complementar

- ABNT NBR ISO 27001 - Segurança da Informação.
- Lei Nº 12.965, de 23 de abril de 2014 – Marco Civil da *Internet*.
- Lei Nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais ("LGPD").

G. Disposições Gerais

Esta Política entra em vigor na data de sua publicação e revoga quaisquer documentos em contrário.

São Paulo, 01 de Agosto de 2024

Beephish Treinamentos e Capacitação LTDA.