Política de Segurança da Informação

Sumário

1. Segurança da Informação

O objetivo dessa política é de regulamentar e disciplinar os procedimentos de coleta e guarda de informações, bem como as regras relativas à segurança e eventual disponibilização destas, em caso de requisição nos termos da legislação aplicável, de forma a minimizar os riscos sobre os ativos de informação, incluindo pessoas, ambientes, tecnologias e processos.

A informação é um ativo de extremo valor e importância, sendo um elemento fundamental para o sucesso dos negócios, portanto, deve ser adequadamente protegida, de forma a garantir a manutenção da confidencialidade, integridade e disponibilidade dos dados.

Esta Política aplica-se a todos os colaboradores da Foco Atuarial.

2. Princípios da Segurança da Informação

Confidencialidade: garantir que a informação não estará disponível ou será divulgada a indivíduos, entidades ou aplicativos sem autorização, ou seja, garantir que determinada informação, fonte ou sistema é acessível apenas às pessoas previamente autorizadas a terem acesso. Garantir o resguardo das informações dadas em confiança e proteção contra a sua revelação não autorizadas.

Integridade: garantir que a informação não tenha sido alterada em seu conteúdo e, portanto, é íntegra, autêntica, procedente e fidedigna. Uma informação íntegra é uma informação que não foi alterada de forma indevida ou não autorizada.

Disponibilidade: permite que a informação seja utilizada quando necessário, portanto, deve estar ao alcance de seus usuários e destinatários e pode ser acessada quando for necessário utilizá-la.

3. Proteção de Dados Pessoais e Sensíveis

Mantemos nossos processos atualizados para proteção de dados pessoais e sensíveis, de forma que as medidas de segurança são essenciais para garantir o cumprimento da legislação vigente.

4. Segurança Física e do Ambiente

A segurança física dos ambientes tem por objetivo prevenir o acesso físico não autorizado, danos às instalações, fraude ou sabotagem entre outras ameaças.

5. Segurança da Informação

A Segurança da Informação está pautada no alinhamento sistemático de ações que visam proteger as informações de negócio dos mais variados tipos de ameaças, garantindo desta forma, a continuidade do negócio, mitigação de riscos, maximização do retorno sobre os investimentos e aumentando as oportunidades de negócio.

Possuímos um programa contínuo de gestão e segurança da informação junto à Microsoft Office e prestador de serviço estabelecido para garantir um ambiente seguro, embasado nos princípios da confidencialidade, integridade e disponibilidade das informações e serviços oferecidos.

6. Utilização aceitável

Os recursos de TI corporativos devem ser usados para fins profissionais. O uso pessoal ocasional e limitado é permitido se não interferir no desempenho e produtividade do trabalho e estiver de acordo com as diretrizes pertinentes à utilização dos recursos de TI disponibilizados pela companhia.

Tais recursos (merecendo destaque a navegação na internet, os e-mails corporativos, as linhas telefônicas e os aplicativos corporativos, inclusive os de trocas de mensagens) estão sujeitos a controle e monitoramento, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, visando resguardar a segurança das informações e dos próprios colaboradores

É proibido o acesso a websites e o armazenamento de arquivos relacionados a pornografia, pornografia infantil, jogos de azar, drogas, violação de direitos autorais, violação de propriedade intelectual, conteúdos discriminatórios, difamatórios ou que depreciem qualquer indivíduo ou entidade, materiais ilícitos/criminosos e qualquer outro que possa ferir a legislação.

O e-mail é uma ferramenta de comunicação profissional, que todos os funcionários devem usar de maneira responsável, eficaz e legal.

7. Estação de Trabalho

- As estações de trabalho incluem laptops e desktops e possuem as seguintes regras de uso:

- Não é permitido que usuários não autorizados acessem sua estação de trabalho;
- Mantenha os devidos cuidados com seu equipamento de trabalho;
- Não é permitido instalar ou desinstalar nenhum software sem autorização do time de Tecnologia da Informação;

- O usuário deve bloquear seu equipamento quando se ausentar da sala e desligá-lo no final do expediente ou em ausências prolongadas.

8. Gestão de Identidade e Controle de Acesso

Os processos de concessão, alteração e exclusão de acesso aos ativos de informação, sistemas de informação e/ou ambientes são realizados pelo time de Tecnologia da Informação, mediante aprovação formal do gestor do solicitante e do respectivo proprietário do sistema e/ou perfil, sempre quando necessário para o desempenho das atividades.

Os acessos privilegiados que implicam em responsabilidades adicionais ao usuário são concedidos com critérios mais rígidos, mediante o cumprimento de regras específicas:

- Gerenciamento de privilégios: hierarquias claras devem ser determinadas para cada sistema e cada hierarquia deve ser formalmente aprovada pelo Time de Tecnologia;

- Gerenciamento de usuários: cada sistema deve ter procedimentos claros para aprovação e método de concessão de acesso a esse sistema com trilhas de auditoria; e os direitos de acesso do usuário estão sujeitos a revisões periódicas.

9. Credenciais de Acesso (Usuário e Senha)

Para acesso aos nossos dispositivos e sistemas deverão ser exigidas senhas de acesso dos Usuários. A senha é de responsabilidade de cada usuário, que deve considerar as seguintes regras:

- A senha é pessoal e intransferível, não devendo ser compartilhada. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que o exercido por outro indivíduo e/ou organização de posse da sua conta de acesso;
- Não salvar em navegadores da web;
- Não devem ser anotadas ou armazenadas em meios físicos ou digitais (e-mail, planilhas, bloco de notas, arquivos na rede, dentre outros);
- Se desconfiar que elas tenham sido descobertas ou acontecer algo com um equipamento como roubo ou perda, solicitar alteração e/ou bloqueio imediato;
- Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível. Já os usuários

que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente;

- Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a equipe de tecnologia;
- A periodicidade máxima para troca das senhas é 180 (cento e oitenta) dias, não podendo ser repetidas as 3 (três) últimas senhas;
- Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários;
- Os sistemas e computadores devem ter versões do software antivírus instalados, ativados e atualizados permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável;
- Contamos com serviço de dupla autenticação que deve ser ativado sempre que disponível.

10. Backups

As realizações de Backups deveram ser feitas conforme o Plano de Continuidade de Negócios (PCN), juntamente a equipe de TI.

11. Plano de continuidade do negócio

Conforme o documento Plano de Continuidade de Negócios (PCN), feito para a Foco Atuarial.

12. Penalidades

A matéria tratada nesta Política é pautada na legislação brasileira vigente, especialmente na Constituição Federal, Código Civil, Código Penal, Consolidação das Leis do Trabalho (CLT), Lei nº 9.279/96 (Propriedade Industrial), Lei nº 9.610/98 (Direitos Autorais), Lei nº 9.609/98 (Software), Lei nº 13.709/18 (LGPD) e demais legislações aplicáveis.

A violação das regras definidas nesta Política poderá acarretar penalidades de acordo com a gravidade da falta cometida, inclusive rescisão contratual, independentemente do regime jurídico a qual o colaborador ou o prestador de serviço estava submetido.

Assim como a ética, a segurança deve ser entendida como parte fundamental da nossa cultura, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição. Assim como o Documento de Código de ética feito para a Foco Atuarial.

16.Disposições Gerais

Esta política vigorará por tempo indeterminado, ou até que seja formalizado e/ou divulgado eventuais modificações, substituições e/ou consolidações.

17.Histórico e Atualizações

VERSÃO	DATA	CONTEÚDO
01	18/09/2023	Elaboração do documento.

18.Aprovações

ELABORAÇÃO	REVISÃO	APROVAÇÃO
Map&An Digital and Financial Services		