Política de Segurança Cibernética

1. Sumário

1. DEFINIÇÃO

A Política de Segurança Cibernética tem como objetivo apresentar os critérios que norteiam a FONTECRED SCD no controle e proteção de seus ativos e dados, de forma a garantir a disponibilidade, integridade e confidencialidade das informações necessárias para a realização de seus negócios.

2. DISPOSIÇÕES GERAIS

A Política é aplicável a todos os funcionários da empresa ou aos que direta ou indiretamente estão vinculados à empresa, cabendo a todos zelar pela confidencialidade e integridade das informações e ativos. Esses dados são de propriedade e uso exclusivo da empresa, sendo vedada sua divulgação a terceiros sem que haja autorização prévia.

3. PRINCIPAIS CONCEITOS

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos, incluindo os controles relacionados aos serviços de nuvem contratados.

- **Confidencialidade**: garantia de que a informação é acessível somente as pessoas autorizadas.
- **Integridade**: salvaguarda da exatidão e dos métodos de processamento da informação.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.
- **Riscos Cibernéticos**: riscos de ataques cibernéticos, internos ou externos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDos e Botnets), sabotagem, bem como violação de acessos e privacidade, que podem desproteger dados, redes e sistemas da empresa causando danos financeiros e de reputação ou imagem.

4. CRITÉRIOS

4.1 Controle do acesso físico

Os acessos ao andar são monitorados por câmera. Também são controlados por CFTV os acessos o andar e ambientes de acesso restrito por meio de uso de biometria. O acesso às dependências da empresa ocorre por meio de sistema de biometria.
O cadastro da biometria é realizado pela área de TI, quando da entrada do colaborador. No desligamento do colaborador, os acessos são bloqueados imediatamente pela área de TI.

4.2 Controle do acesso lógico

As senhas de acesso à rede e sistemas são de uso pessoal e intransferíveis, sendo que cada colaborador é responsável pela proteção e guarda de acesso de uso próprio. É vedado o compartilhamento de senha. O acesso às aplicações é controlado por controle de usuários, feito pelo TI.

Para monitorar a infraestrutura de rede é utilizado ferramenta da Cisco e UniFi Controller.

Cabe a área de TI estabelecer os acessos ao sistema e informações que cada colaborador precisa ter, atribuindo o perfil adequado às funções exercidas. Todas as senhas expiram após um mês. Em caso de transferência, é realizado adequação no perfil. Em caso de desligamento de funcionário, os acessos são bloqueados. Em caso de vazamento de informações, os procedimentos internos adotados são de mitigação dos riscos e tomar todas as medidas cabíveis.

4.3 Concessão de aparelhos eletrônicos

A aquisição de aparelhos eletrônicos é de responsabilidade da área de Tecnologia. Os usuários que tiverem direito ao uso de equipamentos portáteis (laptop, aparelhos telefônicos), ou qualquer outro aparelho eletrônico, de propriedade da empresa, devem assinar Termo de Responsabilidade pela guarda e uso de equipamento de trabalho (Anexo I) e estar cientes de que:

- Os recursos disponibilizados para os usuários têm como objetivo a realização de atividades profissionais;

- A proteção do equipamento é de responsabilidade do próprio usuário, assim como assegurar a integridade e confidencialidade da informação contida no mesmo;
- O usuário não deve alterar a configuração do equipamento recebido;
- Em caso de roubo ou furto, a ocorrência deve ser registrada junto a uma delegacia de polícia e enviada, imediatamente, ao superior do usuário e à área de TI. Neste caso, os custos provenientes da reposição do equipamento serão de responsabilidade da empresa.

O funcionário é responsável pela integridade dos equipamentos que estiverem sob sua posse, respondendo por qualquer dano gerado, sendo passível inclusive de ser obrigado a realizar a reposição do bem.

Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pela área de TI, via rede, sendo que o usuário não tem a permissão para desabilitar o programa antivírus instalado nas estações de trabalho.

4.4 Licenças de uso

As licenças de software são de inteira responsabilidade da área de TI, sendo que estes devem controlar a quantidade de licenças, as instalações nos equipamentos e as devidas atualizações.

4.5 Uso de e-mail

O e-mail é um instrumento de comunicação interna e externa para a realização dos negócios da empresa, cabendo a cada usuário a responsabilidade pelo seu uso estritamente profissional, devendo inclusive monitorar a linguagem utilizada na comunicação, de forma a não comprometer a imagem da FONTECRED.

4.6 Gestão por modulo

A área de TI é responsável por conceder acesso aos usuários da empresa sendo ela segregada por área:

- Crédito
- Cobrança
- BackOffice
- Master
- Atendimento
- Comercial
- Gestão

Cada área tem seus acessos delimitados, podendo ser acessados de acordo com sua funcionalidade no trabalho.

4.7 Uso de internet

O uso da Internet deve ser exclusivo para assuntos de interesse da empresa, estando sujeito a monitoramento pela área de TI para identificar o usuário conectado, o tempo de conexão e os sites acessados.

Os usuários deverão acessar as redes da empresa de acordo com o uso:

- **CORP_FONTECRED –** Para uso exclusivo de notebook ’s corporativos apenas de funcionários

- **CELULAR_FONTECRED –** Para uso exclusivo de celular corporativos de funcionários.

- **VISITANTE_FONTECRED –** Para uso de visitantes caso precisem e para acesso de celular particular.

4.8 Confidencialidade das informações

Todo colaborador deve manter sigilo absoluto sobre as operações e informações privilegiadas e confidenciais que vierem a obter em função de suas respectivas atividades, tais como prognósticos financeiros ou de negócios, investimentos, estratégias de marketing, pesquisas, exceto se as informações tiverem caráter público ou se tornem públicas e não influenciem nenhuma tomada de decisão. Qualquer informação fornecida a terceiros ou utilizada em benefício próprio, sem a anuência da Diretoria, é passível de responsabilização civil e criminal. Também é vedado.

A divulgação ou prestação de quaisquer informações, ainda que exigidas oficialmente por órgãos competentes, depende de prévia autorização da Diretoria.

4.9 Backup

A área de TI é responsável por gerenciar o banco de dados e arquivos na rede, realizando cópias de segurança. Todas as informações da rede também são armazenadas em nuvem, permitindo guardar dados na internet através de um servidor online sempre disponível.

4.10 Antivírus

A área de TI é responsável por gerenciar todos os ativos da empresa, instalando o Antivírus em todos os equipamentos. Ele é de uso exclusivo para proteção do usuário e de suas informações evitando que o usuário tenha algum malware infectando seu equipamento. A área de TI faz validações periódicas em todos os ativos através do portal com todos os equipamentos e plena funcionalidade.

5. DISPOSIÇÕES FINAIS

Todos os colaboradores devem ter a sua disposição uma cópia desta política e atestar, mediante assinatura do Termo de Responsabilidade, sua aderência às normas aqui apresentadas. Qualquer infração às normas contidas nesta política sujeita seu agente às sanções previstas no Código de Ética e Conduta.

6. ANEXO I

TERMO DE RESPONSABILIDADE - EMPRÉSTIMO DE EQUIPAMENTO

Solicitante: _____

Setor/ Unidade: _____Telefone: _____

Data de retirada: _____ Data de devolução:_____

Local de uso (cidade, estado, país): _____

Equipamento (s): Data: N° de série

1°		
2°		
3°		
4°		
5°		
6°		

Eu _____ portador do RG: _____ e do CPF: _____ declaro utilizar com cuidado e zelo o equipamento solicitado. Afirmo ter verificado, antes da retirada, que o equipamento se encontrava:

() em perfeitas condições de uso e bom estado de conservação

( ) com os seguintes problemas e/ou danos (descrevê-los):