Sumário

1. Objetivo
2. Escopo / Aplicabilidade
3. Diretrizes gerais
4. Papéis & Responsabilidades
5. Anexos
6. Referências
7. Glossário
8. Propósito
9. Política de segurança da informação
10. Códigos maliciosos
11. Antivírus
12. Firewall
13. Senhas
14. Criptografia
15. Backup
16. Código fonte
17. Https:
18. Acordo de confidencialidade
19. Código de Conduta

1. Objetivo

Esta Política de Segurança da Informação contém os requisitos de segurança que visam garantir a segurança da informação em vigor, a fim de proteger as informações da SCC Check e de toda sua rede de associados e parceiros.

2. Escopo / Aplicabilidade

Aplicável a todos as frentes de negócio da SCC Check

3. Diretrizes Gerais

Esta Política define as diretrizes para a Segurança da Informação, visando definir os requisitos mínimos para garantir a integridade, confidencialidade e disponibilidade das informações compartilhados pela SCC Check com os seus clientes finais, fornecedores e colaboradores, identificados como USUÁRIOS

O Programa de Avaliação de Segurança é dividido em fases conforme abaixo:

Planejamento - Elaboração da agenda anual das avaliações;

Coleta de dados - Envio de questionário de avaliação criado de acordo com a necessidade;

Execução - Análise do ambiente com entrevistas que serão realizadas com os profissionais de tecnologia para a obtenção do entendimento da infraestrutura e da coleta e análise das evidências;

Análise dos resultados - Elaboração de plano de ação com prazo de implementação;

Comunicação dos resultados - Envio dos resultados para as partes envolvidas;

Monitoramento - Follow-up de implantação das ações necessárias.

Todas as avaliações são baseadas na Política de Segurança em linha com as melhores práticas do mercado.

4. Papéis & Responsabilidades

O usuário deverá implementar e manter os requisitos de Segurança da Informação apropriados ao seu tamanho e complexidade, a natureza e o alcance de suas atividades, e a sensibilidade da informação fornecida a ele pela SCC Check. Tais garantias deverão incluir os elementos estabelecidos nos Controles de Segurança especificados neste documento, e devem ser implementados para garantir a segurança e confidencialidade das informações fornecidas pela SCC Check. Esses controles visam proteger a integridade das informações contra quaisquer ameaças e/ou riscos, protegendo-as contra o acesso não autorizado e/ou o uso de tais informações de forma indevida.

A SCC Check terá o direito de auditar o usuário para assegurar a implementação dos controles de segurança previstos nesta política. A SCC Check será responsável por assegurar a plena cooperação de seus Provedores Técnicos, em conexão com as auditorias.

O usuário deverá responder imediatamente ou no prazo previamente estabelecido, de acordo com a tabela abaixo, todas as fases relacionadas na auditoria de Segurança da Informação.

O não atendimento dentro do período acordado poderá submeter o usuário às sanções previstas em contrato.

Fase	Prazo para resposta
Coleta de Dados / Questionário	10 dias
Comunicação dos resultados / Aceite do plano de ação	10 dias
Monitoramento / Evidências	De acordo com o plano de ação

5. Anexos

Guia Prático de Segurança da Informação

6. Referências

Todas as avaliações são baseadas na Política de Segurança em linha com as melhores práticas do mercado.

7. Glossário

Controles de Segurança

Antivírus
Aquisição de solução de antivírus comercial, para prover proteção para equipamentos (desktops, servidores, tablets e notebooks), licença de uso de software, implantação e garantia de atualização contínua.

Firewall
Os firewalls são dispositivos que controlam o tráfego externo via computador implementados na rede da empresa. Sua função consiste basicamente em bloquear o tráfego em áreas mais críticas dentro da rede interna e liberar acessos bem-vindos. Todos os sistemas devem ser protegidos contra o acesso não autorizado através da Internet, seja ele via e-commerce, acesso dos funcionários com base na Internet e via browsers, ou acesso via e-mail de funcionários. O firewall é o principal mecanismo de proteção de qualquer rede de computadores.

Backups
Os backups devem fazer parte da rotina de operação dos seus sistemas baseando-se numa política determinada. A existência de uma política de backup em sua empresa tem como objetivo armazenar informações valiosas, levando em consideração a segurança e integridade dos dados, para que em caso de necessidade seja possível recuperá-los.

Política de backup: Define as regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução;

Backup criptografado: Você deve armazenar dados sensíveis (informações do banco de dados, informações dos clientes; código fonte da aplicação e etc.) em formato criptografado,

Implementar criptografia nos Backups para não correr o risco do uso indevido de informações sigilosas.

Site HTTPS

O site do usuário deve implementar a utilização do protocolo de comunicação HTTPS, em regra, quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros. Através deste protocolo, os dados são transmitidos por meio de uma conexão criptografada, criando um canal seguro com alto nível de proteção para as suas informações sensíveis.

Ambiente Compartilhado

Empresas do mesmo segmento que prestam serviços de informações, desde que esses não sejam iguais ou que tenham alguma semelhança com aqueles oferecidos pela SCC Check e seus fornecedores, não podem ter o ambiente tecnológico compartilhado.

Armazenamento do "resultado" da consulta realizada

Absolutamente vedado o armazenamento do relatório gerado e fornecido ao usuário. Reter esses dados para quaisquer fins é considerado violação de contrato e pode ser caracterizado como fraude cabível de multa e destrato.

Log

Data, Hora e IP: Deverá manter armazenados os logs de operações como registro da data, da hora, da identificação, inclusive do “Internet Protocol”- IP do consulente quando executada a consulta, mantendo-os à disposição da SCC Check.

Troca de Senhas: Deverá manter armazenados os logs de quando é realizada a troca de senha do usuário. Não ter o registo no log torna impossível afirmar que os usuários realizam a troca de senha regularmente.

A tabela no banco de dados da aplicação que armazenam o logon e a senha dos usuários devem ser criptografadas;

Senhas e logons em texto limpo ficam vulneráveis para serem visualizadas, comprometendo assim a segurança das informações. O usuário deverá manter criptografado os dados confidenciais dos usuários, aumentando seu nível de segurança.

É de responsabilidade do usuário zelar integralmente pela segurança e confidencialidade das informações dos seus clientes.

Usuário e senha de conexão com a SCC Check devem ser protegidos com Controle de Acesso e Criptografia;

O usuário e senha de conexão via string com a SCC Check devem ser protegidos no ambiente tecnológico com um conjunto de procedimentos e medidas, a fim de resguardar ambas as partes contra tentativas de acesso não autorizadas.

É de responsabilidade do usuário zelar integralmente pela segurança e confidencialidade do usuário e senha de conexão com a SCC Check.

Conscientização e aplicação de Política de Segurança da Informação para funcionários e clientes;

O usuário deverá conscientizar e/ou reforçar assuntos de Segurança da Informação que necessitam ser abordados pela comunicação. As boas práticas de Segurança da Informação aplicadas em sua totalidade serão de grande valia para proteção de seus negócios, reduzindo riscos de ataques, comprometimento de informações confidenciais e fraudes.

Terceirização de Serviços;

Ao usar os Provedores de Tecnologia para acessar, transmitir, desenvolver sistemas ou processar dados, o usuário deve:

a. Adequar due diligence para manter a conformidade com as leis e regulamentos aplicáveis e obrigações contratuais;

b. Estabelecer contratos de Confidencialidade / NDA (Non Disclosure Agreement), obrigação de Confidencialidade dos Provedores de Tecnologia;

c. Considerar que os processos desses prestadores de serviços também serão escopo da avaliação de segurança realizado pela SCC Check;

d. Assegurar que o mesmo prestador de serviços não possua contrato semelhante com outro empresa do mesmo setor da SCC Check.

Para que os usuários possam utilizar meio de acesso Logon Master é necessária a troca de senha periódica;

É recomendado implementar uma troca de senha ao usuário Logon Master para evitar o vazamento da senha e a ocorrência de fraudes.

Continuidade de Negócios e Recuperação de Desastres;

Em caso de sinistro é de responsabilidade do usuário um nível de atendimento/suporte mínimo para seus clientes.

Segurança Física.

Responsabilidade do usuário implementar controles que minimamente protejam a integridade física do ambiente da empresa, tais como:

i. Definição dos controles necessários para uma dependência segura;

ii. Controle de acesso físico às áreas restritas (ex.: sala de servidores).

8. Propósito

A SCC Check está comprometida em assegurar a disponibilidade, a integridade e a confidencialidade das informações compartilhadas com parceiros de negócios.

Pequenas e médias empresas são mais vulneráveis ao crime eletrônico e incidentes de Segurança da Informação, pois geralmente possuem uma estrutura robusta para manter sistemas e informações adequadamente protegidos.
Este guia foi desenvolvido para divulgar os requisitos mínimos de segurança da informação que sua empresa necessita implementar para estar em conformidade com os padrões de Segurança da

Informação recomendados pela SCC Check para atender nossos clientes e parceiros de negócio de forma adequada e segura.

9. Política de segurança da informação

É um documento que apresenta as boas práticas adotadas pela empresa para nortear a segurança da informação. Sua adoção por todos os colaboradores é primordial. As boas práticas indicam que toda companhia deve criar regras sobre como todos os colaboradores devem lidar com a proteção das informações da empresa, incluindo os dados e informações de seus clientes e parceiros de negócios. O conteúdo deve ser disseminado entre todos, e explicado no momento da contratação. Recomenda-se solicitar a assinatura de um termo de compromisso para o cumprimento das normas.

10. Códigos maliciosos

Códigos maliciosos, também conhecidos como malwares, são usados como intermediários e possibilitam a prática de golpes, a realização de ataques e o envio de spam. São programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador.
Um usuário mal-intencionado pode instalar um código malicioso no seu computador, após invadir sua rede ou explorar alguma vulnerabilidade existente seu ambiente.

Seu ambiente de tecnologia também pode ser infectado caso você:

- Acesse páginas maliciosas na Internet, usando navegadores vulneráveis;
- Acesse mídias removíveis infectadas, como pen-drives;
- Execute arquivos infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas na Internet, redes sociais ou diretamente de outros computadores.

Após infectar o seu computador, o código malicioso pode executar ações como se fosse você, tais como: acessar informações confidenciais, apagar arquivos, conectar-se à Internet, enviar mensagens e/ou instalar outros códigos maliciosos.
Outros dispositivos também podem ser infectados por códigos maliciosos: tabletes e smartphones, por exemplo.

<u>Tipos principais de vírus.</u>
Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Cavalo de Tróia (trojan)
Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.
Rootkit
Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
Backdoor

Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

Worm

Programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de computador para computador.

Bot

Programa similar ao worm e que possui mecanismos de comunicação com o invasor que permitem que ele seja remotamente controlado. Zumbi é como é chamado um computador infectado por um bot, pois pode ser controlado remotamente, sem o conhecimento do seu dono. Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

Spyware

Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Keylogger

É um tipo de spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

Screenlogger

É um tipo de spyware, similar ao keylogger, usado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking.

Adware

É um tipo de spyware projetado especificamente para apresentar propagandas.

11. Antivírus

O Antivírus é um software essencial que protege os computadores e suas informações de diferentes tipos e níveis de ataques maliciosos.

É extremamente importante certificar-se de que este programa é atualizado pelo menos uma vez por semana, não basta apenas ter um antivírus instalado no computador, é preciso mantê- lo atualizado e seguro para que não haja problemas na sua rede. Mesmo porque, quando seu computador é infectado por vírus há grande chance de perder documentos e arquivos importantes, além da possibilidade de indisponibilidade do seu sistema.

Dicas:

- Escolher e selecionar um antivírus de renome;
- Não utilizar antivírus sem licença;
- Estar sempre com o programa e as proteções atualizadas;
- Executar uma varredura periodicamente completa de seu sistema;
- Manter-se longe a pirataria de software dos seus computadores e da sua rede;
- Utilize o antivírus antes de abrir arquivos baixados da internet, anexos, ao conectar mídias em seu computador e pen-drives.

12. Firewall

Um firewall é um sistema de proteção de um computador ou de uma rede de computadores contra ataques provenientes de diferentes redes (principalmente da Internet). O Firewall verifica cada pacote recebido e decide se o mesmo pode ser enviado ao destino ou se deve ser barrado, de acordo com parâmetros de segurança definidos.
Dicas:

- Adquirir e manter atualizado um programa firewall ou um dispositivo de firewall;
- Implementar regras a política de segurança da rede em questão;
- Fazer registros de log de todos os eventos suspeitos;
- Emitir alertas sobre tentativas que comprometem a política de segurança.

13. Senhas

Contas e senhas são os principais mecanismos de autenticação utilizados. Por meio de contas e senhas os sistemas conseguem saber quem você é, confirmando sua identidade e definindo as ações que você pode realizar.
Proteger a sua identidade virtual (conta e senha) é essencial para proteger o acesso às informações e a segurança do sistema, prevenindo riscos de alteração indevida, vazamento de informação e indisponibilidade do sistema. A confidencialidade assegura a sua identidade.

Se uma outra pessoa souber a sua conta de usuário e tiver acesso à sua senha, ela poderá usá- las para se passar por você na Internet, e/ou nos demais sistemas, e você poderá ser responsabilizado pelos acessos.

Algumas das formas como sua senha pode ser indevidamente descoberta são:

- Quando usada em computadores infectados
- Quando usada em computadores invadidos
- Quando usada em sites falsos
- Por meio de tentativas de adivinhação (principalmente, quando a senha é fraca, ou seja, de fácil adivinhação)
- Ao ser capturada enquanto trafega na rede
- Por meio do acesso ao arquivo onde foi armazenada
- Com o uso de técnicas de engenharia social pela observação da movimentação dos seus dedos no teclado

Algumas das ações que um invasor pode realizar, caso tenha acesso às suas senhas, e os riscos que estas ações podem representar são:

- Ler e/ou apagar seus e-mails
- Furtar sua lista de contatos e enviar e-mails em seu nome
- Enviar mensagens de spam e/ou contendo phishing e códigos maliciosos
- Pedir o reenvio de senhas de outras contas (e assim conseguir acesso a elas)
- Trocar sua senha, dificultando que você acesse novamente sua conta
- Apagar seus arquivos e obter informações sensíveis, inclusive outras senhas, instalar códigos e serviços maliciosos

- Acessar redes sociais e denegrir a sua imagem e explorar a confiança de seus amigos/seguidores
- Enviar mensagens de spam ou contendo boatos e códigos maliciosos
- Alterar as configurações feitas por você, tornando públicas informações privadas
- Acessar sua conta bancária e verificar seu extrato e seu saldo bancário
- Acessar seu site de comércio eletrônico e alterar informações de cadastro, fazer compras em seu nome e verificar informações sobre suas compras anteriores.

Evite usar:

- Dados pessoais, como nomes, sobrenomes, contas de usuário, datas, números de documentos, placas de carros e números de telefones, dados que possam ser obtidos em redes sociais e páginas na Internet, sequências de teclado, como “1qaz2wsx” e “QwerTAsdfG”, palavras que fazem parte de listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes e dicionários de diferentes idiomas.

Recomendamos:

- A senha deve ser pessoal e única para cada usuário.
- Não compartilhe sua senha com ninguém.
- Combinar letras, números e símbolos (ex.: @, #, $) para formar sua senha;
- Utilizar o máximo de caracteres permitidos (quanto maior a senha, mais difícil para ser “quebrada” por pessoas mal-intencionadas).
- Troque suas senhas regularmente
- Utilize senhas diferentes para sistemas importantes (bancos, e-mails, sites,etc).
- Não compartilhe sua senha com ninguém.
- Nunca anotar sua senha em agendas, arquivos, post-its ou em lugares a que outras pessoas possam ter acesso. O indicado é memorizá-la.

14. Criptografia

As senhas desses usuários geralmente estão entre as informações mais valiosas que se pode obter desses serviços, portanto, armazená-las em um local de fácil acesso (ex. formato texto) é uma atitude irresponsável dos desenvolvedores desses serviços.
A incorporação de recursos de segurança, principalmente a criptografia, é a prática mais recomendável para a proteção das suas senhas e de seus clientes.

15. Backup

Um backup não serve apenas para ser usado no lugar de um arquivo danificado ou inacessível. A cópia também pode ser usada para consultar informações. Por isso, é importante ter em mente qual a finalidade do arquivo e com que frequência ele é atualizado para definir o intervalo no qual as cópias de segurança devem ser feitas.

Guardar os arquivos em local seguro e efetuar backup periódico é o nível de segurança mais simples e barato para garantir um mínimo de contingência para seu sistema, em caso de algum evento que possa impactar o serviço.
As empresas precisam ter a preocupação de armazenar em segurança todas as informações envolvidas no contexto da organização. Lembrando que as informações são bem mais valioso da empresa, principalmente se estas informações estão armazenadas em bancos de dados, é fundamental ter uma estratégia bem definida para a proteção deste bem tão valioso.
Devemos nos preocupar não apenas com a perda dos dados, mas também com acessos indevidos, alterações não autorizadas e/ou roubo de informações.

Alguns exemplos:

- Invasões e ataque de hackers;
- Acesso indevido às informações;
- Desastres naturais;
- Incêndios;
- Inundações;
- Alterações indevidas (quebra de integridade);
- Falhas de hardware.

Um importante fator que devemos levar em consideração, na hora de montarmos a nossa estratégia de backup/restore é a proteção dos dados. Se a informação a ser protegida tem valor estratégico para a empresa, é vital que os dados precisam estar disponíveis e bem protegidos, dessa forma, mesmo que os custos para proteção sejam elevados, serão facilmente justificáveis.
Lembramos ainda que, não basta fazer o backup, precisamos de uma estratégia de testes e simulação de restauração dos dados, pois muitas vezes, apesar do procedimento de backup ser realizado com sucesso, no momento de restaurar os dados é que se verificam os problemas. Por isso, uma prática recomendável, é realizar uma rotina de testes periódicos de restauração dos dados de backups como parte da estratégia de segurança.

16. Código fonte

Na busca por melhor desempenho e controle de suas operações, as empresas têm investido cada vez mais em softwares, que se tornam essenciais para gerir o negócio. Adquirir um software feito sob medida é uma atividade de grande risco. Não apenas porque o programa deverá se encaixar o mais perfeitamente possível às necessidades da empresa, mas porque esse software vai criar uma dependência com o desenvolvedor, incluindo manutenções, reparos e atualização de novas tecnologias e necessidades. Se o desenvolvedor falir ou encerrar suas atividades, ou mesmo em casos de desacordo comercial, o negócio poderá ser grandemente afetado.
Ao se contratar uma empresa para desenvolvimento de software, o adquirente poderá exigir por contrato, que o código-fonte seja entregue aos cuidados de um terceiro de confiança das partes (terceiro depositário). O contrato deve prevê as condições nas quais o adquirente pode reivindicar o código-fonte do software, caso o adquirente não poder contar mais com a assistência do desenvolvedor poderá utilizar sua equipe de TI própria ou até mesmo contratar outra empresa de desenvolvimento para dar

manutenção ao programa. Isso diminui consideravelmente o risco de prejuízos oriundos da interrupção do funcionamento do software.
O terceiro depositário precisa ser de confiança de ambas as partes, idôneo e com experiência no ramo. Isso porque o código-fonte é a alma do software, objeto de proteção da lei de direitos autorais. Se uma pessoa de má-fé se apropriar dele, poderá reproduzir o programa livremente, o que gerará grandes prejuízos à empresa. É conveniente também verificar o nível de segurança da informação oferecido, já que a ação de hackers poderia fazer vazar as informações estratégicas.
O acesso ao código-fonte do programa deve ser controlado, com a finalidade de prevenir a introdução de funcionalidades não autorizadas e para evitar mudanças não intencionais.

Os seguintes requisitos de segurança da informação devem ser considerados para o controle de acesso ao código fonte, com a finalidade de reduzir o risco:

- Manter o acesso restrito ao código-fonte;
- Manter o código-fonte em um ambiente seguro;
- Manter um registro de auditoria de todos os acessos e alterações ao código-fonte.

17. Https:

O HTTPS (Hyper Text Transfer Protocol Secure) é o protocolo ou conjunto de regras e códigos com uma camada de segurança que torna a navegação mais segura. Essa camada adicional de segurança permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais

O HTTP (protocolo normal) não oferece a mesma segurança do HTTPS porque as informações navegam na rede de uma forma muito parecida com a apresentada na tela ou digitadas pelo usuário. Por exemplo, se o usuário digita um login "xxx" e uma senha "1234", essa informação é enviada através de pacotes de dados pela rede. Alguém pode interceptar esses dados no meio do caminho e acessar informações confidenciais de forma não autorizadas.
Interceptar pacotes entre a origem e o destino não é muito complicado na internet. Eles passam por diversas redes de uma ponta até a outra, como a rede de nossa casa ou empresa, a rede do nosso provedor e a rede onde está o servidor de Internet, por exemplo. Em qualquer desses pontos um indivíduo mal-intencionado pode encontrar meios de visualizar os pacotes de dados que trafegam.

18. Acordo de confidencialidade

Os acordos de confidencialidade podem preceder não apenas eventos estratégicos, como parcerias comerciais, avaliações para aquisição de empresa ou o desenvolvimento conjunto de um produto, mas também eventos corriqueiros, como a contratação de serviços ou a realização de uma grande compra, hipóteses nas quais o fornecimento de informações pode ser necessário para a execução do serviço ou para a cotação junto ao fornecedor. Em qualquer dessas hipóteses a atenção deve ser a mesma, pois a importância desta espécie de acordo não está relacionada com o projeto ao qual ele está vinculado, mas com a proteção da informação estratégica.

Este acordo é um controle administrativo extra judicial que impõem a aplicação da confidencialidade entre contratada e contratante sobre as informações envolvida em um contrato de prestação de serviços.

19. Código de Conduta

Este é o Código de Conduta da SCC CHECK foi instituído pela Diretoria, em especial, sob a liderança do Diretor Administrador da SCC CHECK.

O Código aborda, em linhas gerais, os valores que orientam a empresa SCC CHECK.
Não tem a pretensão de ser completo nem detalhista. É sim, um documento para orientar a conduta pessoal e profissional dos administradores, funcionários, estagiários e prestadores de serviços regulares da SCC CHECK, devendo ser considerado como uma declaração formal do compromisso dos Colaboradores da SCC CHECK com as regras de ética empresarial e social, bem como com princípios da transparência, respeito à igualdade de direitos, à diversidade e prestação de contas, devendo ser plenamente cumprido por todos, tanto interna quanto externamente.

PRINCÍPIOS GERAIS

A SCC CHECK é uma empresa socialmente responsável, inserida na comunidade, que constrói sua imagem com base nos seguintes princípios:

- Ética e transparência na condução de seus negócios;
- Qualidade e eficiência de seus serviços;
- Respeito com prática em seus relacionamentos internos ou externos, com a permanente busca por melhoria na qualidade de vida de todos com os quais se relaciona;
- Confidencialidade no trato de informações e dados de seus clientes;
- Responsabilidade no gerenciamento de seu patrimônio físico.

REGRAS DE CONDUTA
As regras de conduta explicitadas neste Código visam a deixar claros Procedimentos e Atitudes eticamente aceitos. Para a SCC CHECK é eticamente aceita a postura profissional que respeita os princípios anteriormente descritos e que não coloca em risco a credibilidade da instituição.
Dessa forma, é vedado aos Colaboradores da empresa:

- Realizar operação nos clientes administrados pela SCC CHECK, em seu nome ou em nome de parentes e amigos, sem observar as regras específicas dispostas neste Código;

- Empregar informações de que disponha em virtude de suas atividades, beneficiando a si próprio ou a terceiros em operações nos clientes administrados pela SCC CHECK;
- Receber comissão, abatimento e/ou favor pessoal, valendo-se de seu cargo ou de sua função na empresa;
- Auferir ou conceder qualquer forma de reciprocidade, ganho ou vantagem pessoal de instituição financeira ou cliente em geral, valendo-se de seu relacionamento profissional;

- Aceitar presente de quem quer que seja, em razão do cargo ou da função exercida na empresa. Tal proibição não se aplica ao recebimento de brinde que não tenha valor comercial relevante (até R$100,00);
- Manifestar-se publicamente em nome da empresa quando não autorizado ou habilitado para tal;
- Manter comportamento pessoal incompatível com os padrões socialmente aceitos, que possa trazer prejuízos para a imagem da empresa;
- Consumir quaisquer substâncias inebriantes nas dependências da SCC CHECK;
- Usar traje inadequado ao ambiente de trabalho;
- Inadimplir em seus negócios pessoais.

PRÁTICAS ANTI-CORRUPÇÃO E ANTI-SUBORNO

Os Colaboradores tomarão cuidado para não envolver a SCC CHECK em compromissos com partidos políticos, igrejas e outras atividades de cunho sectário. A Empresa e seus Colaboradores, se contribuírem financeiramente em campanhas eleitorais (para partidos ou candidatos), deverão proceder estritamente de acordo com a legislação vigente, e de forma transparente. Colaboradores devem informar seu superior imediato sobre contribuições financeiras feitas a campanhas eleitorais, inclusive o montante doado.

RELAÇÕES COM FORNECEDORES

Todos os fornecedores têm a garantia de que seus produtos serão tratados pela empresa com base exclusivamente em critérios mercadológicos e de qualidade, não havendo interferência de qualquer aspecto que possa caracterizar privilégio ou discriminação. Será assegurado ao fornecedor que se sentir prejudicado por qualquer Colaborador da empresa a possibilidade de reportar a ocorrência diretamente à Diretoria da SCC CHECK.
De modo a garantir as premissas explicitadas neste Código de Conduta, todos os Colaboradores, funcionários ou não, estão expressamente proibidos de:

- manter relação comercial, como representante da empresa, com empresa em que ele próprio ou familiar tenha interesse ou participação direta ou indireta, sem autorização do superior hierárquico, em nível de Diretoria ou seu equivalente;

- manter relação comercial com fornecedor da empresa, caso seu cargo ou sua função lhe dê poderes para definir e/ou escolher esse tipo de fornecedor.
Qualquer relação comercial com fornecedor deverá ser prévia e obrigatoriamente comunicada, por escrito, ao respectivo superior e a Diretoria da SCC CHECK;
- aceitar benefício pessoal, como pagamento em dinheiro ou mercadoria, viagem, almoço, jantar ou qualquer vantagem advinda de relacionamento com fornecedor. Despesas com viagem, hospedagem e refeições devem sempre ser pagas pela empresa, mesmo que o convite parta do fornecedor.
No caso dos Colaboradores que atuam na Diretoria Administrativa, não são considerados presentes os produtos recebidos a título de amostra para análise comercial, que devem permanecer no âmbito da SCC CHECK e ser devolvidos ao fornecedor tão logo se conclua por sua aquisição ou não.

RELAÇÕES COM PÚBLICO INTERNO E SEU AMBIENTE

1. Relacionamento no Ambiente de Trabalho

A Política de Recursos Humanos da SCC CHECK é pautada por justiça, transparência, imparcialidade e profissionalismo. Todos os Colaboradores da empresa devem estabelecer no ambiente de trabalho relacionamentos de cortesia e respeito, para que seja possível construir vínculos de lealdade e confiança, bem como espírito de equipe e busca por resultados.

Uma pessoa que tenha envolvimento sentimental ou relação de parentesco com outra deverá se abster de praticar qualquer ato, participar de qualquer processo ou exercer influência sobre pessoas responsáveis por decisões de que possam resultar um benefício pessoal para a pessoa com quem possua relações dessa natureza.

Não são aceitáveis as seguintes condutas:

- Praticar qualquer discriminação em relação à cor, raça, credo religioso, sexo, preferência sexual, idade, etc., nos processos de recrutamento e seleção, treinamento, remuneração, promoção, transferência ou outro fator relacionado ao ambiente de trabalho;
- Contratar parentes sem a expressa concordância da Diretoria, bem como indicar sua contratação ou levar outra pessoa a fazê-lo, sem informar o fato ao responsável pela contratação;
- Usar equipamentos e outros recursos da empresa para fins particulares não autorizados;
- Envolver-se em atividades particulares não autorizadas, que interfiram no tempo de trabalho dedicado à empresa;
- Usar o cargo ou a função para solicitar favores ou serviços pessoais a subordinados;
- Tomar qualquer decisão que afete a carreira profissional de Colaboradores com base apenas em relacionamento pessoal.

Todas as avaliações de desempenho funcional devem ser pautadas por mérito, de modo a propiciar igualdade de acesso às oportunidades de desenvolvimento profissional existente, segundo as habilidades, competências e contribuições de cada profissional.

2. Segurança e Saúde

A SCC CHECK está comprometida em proporcionar um ambiente de trabalho seguro e saudável a seus Colaboradores e visitantes, adotando medidas que evitem a degradação do meio ambiente e que minimizem o impacto de suas atividades.

Cada Colaborador tem a responsabilidade de zelar por procedimentos seguros de operação, que devem garantir sua própria saúde e a de seus colegas de trabalho.

É vedado adotar qualquer comportamento que possa representar risco para a integridade física dos demais Colaboradores.

Para garantir condições de trabalho seguras e sadias é preciso também atitudes responsáveis no cumprimento de leis e normas internas relativas à medicina e à segurança do trabalho.

3. Prestação de Serviços a Terceiros

Os Colaboradores não podem, em princípio, exercer atividade remunerada paralela à exercida na empresa SCC CHECK. Poderão ser admitidos e tratados como exceção os casos em que:

- A natureza do trabalho seja distinta daquela exercida na empresa;
- A atividade não seja exercida durante o período de trabalho e não afete o desempenho do Colaborador na empresa, e tampouco utilize infraestrutura e/ou informações desta ou de seus participantes.

Em qualquer caso, há necessidade de autorização específica da Diretoria da área. O exercício de atividade não remunerada, tal como a participação em entidades filantrópicas, deve ser informado ao superior hierárquico do Colaborador.

RELAÇÕES COM OS FUNCIONÁRIOS DOS CLIENTES

Os Colaboradores da SCC CHECK devem atender a todos os nossos clientes com cortesia, presteza e eficiência. Qualquer dúvida quanto à conveniência de se atender a qualquer solicitação deve ser submetida ao superior hierárquico.
Não haverá tratamento preferencial a nenhum cliente, devendo todos os procedimentos obedecer às diretrizes éticas e operacionais da SCC CHECK.

RELAÇÕES COM OS CLIENTES
O relacionamento com todos os clientes deverá ser pautado por profissionalismo. Os Colaboradores não deverão pronunciar-se, nem fazer comentários e insinuações que possam atingir a imagem de terceiros.

RELAÇÕES COM O SETOR PÚBLICO
Não poderá haver oferecimento, direto ou indireto, a nenhuma autoridade ou servidor da administração pública, federal, estadual ou municipal, de qualquer pagamento em dinheiro, presentes, serviços, entretenimentos ou outro benefício.
Constituem exceções os convites para almoços ou jantares de trabalho, e eventos patrocinados pela empresa, como viagens técnicas, congressos, seminários ou comemorações de que a empresa participe.

Todo e qualquer Colaborador, quando estiver representando publicamente a empresa, deve se abster de manifestar opinião sobre atos de funcionários públicos, ou mesmo de fazer comentários de natureza política.

RELAÇÕES COM A COMUNIDADE E O MEIO AMBIENTE
Os Colaboradores devem ter plena consciência das responsabilidades da SCC CHECK para com a comunidade e o meio ambiente, de forma a reforçar sua atuação como empresa cidadã.
Todo Colaborador, no momento em que estiver representando a empresa perante os membros de uma comunidade, deve agir conforme os princípios explicitados neste Código de Conduta, sem preconceitos ou privilégios de qualquer ordem.

PRESERVAÇÃO DA IMAGEM INSTITUCIONAL

A imagem institucional da SCC CHECK é seu patrimônio mais importante, devendo ser construído e preservado permanentemente por todos.
Qualquer ação ou atitude por parte dos Colaboradores, individual ou coletiva, que vier a prejudicar essa imagem é considerada falta grave.

PRESERVAÇÃO DO PATRIMÔNIO FÍSICO
Todos os Colaboradores são responsáveis pela preservação do patrimônio físico da empresa composto pelas instalações e pelos equipamentos necessários à realização de sua atividade, devendo utilizá-los de forma correta e exclusivamente para fins de trabalho.

INFORMAÇÕES CONFIDENCIAIS
Pela natureza de seu negócio, a SCC CHECK lida com informações de várias fontes, de participantes de negociação, de agentes de compensação e/ou de custódia e de clientes.
Essas informações são confidenciais e só devem ser utilizadas para o desempenho das funções de cada Colaborador e somente podem ser divulgadas: (1) por decisão expressa e por escrito da diretoria e (2) por exigência legal ou ordem judicial.
Documentos e outros dados não divulgados aos clientes referentes aos negócios da SCC CHECK especialmente os de ordem financeira, também são confidenciais.

São igualmente confidenciais e de propriedade da SCC CHECK os documentos referentes à especificação de produtos, softwares, hardwares e aplicativos desenvolvidos ou em uso, mesmo que o Colaborador tenha participado de seu desenvolvimento.
Os Colaboradores devem dedicar um cuidado especial às relações entre as áreas operacionais e de auto regulação da SCC CHECK, mantendo a confidencialidade de documentos que não sejam públicos.
Mesmo informações destinadas ao conhecimento público, tanto em seminários para os quais tenham sido convidados Colaboradores da SCC CHECK, quanto em contatos com a imprensa, devem ser cuidadosamente avaliadas antes de divulgadas. É sempre necessário e prudente certificar-se de que não há nenhuma restrição ou sigilo envolvendo o dado ou informação a ser liberada para o público.

INFORMAÇÕES PRIVILEGIADAS
Os Colaboradores não usarão seu cargo, posição ou influência na SCC CHECK para ter acesso a informações privilegiadas e utilizá-las, em benefício próprio, de seus familiares ou de pessoas de seu relacionamento, para realizar transações com valores.
Se algum Colaborador tiver alguma dúvida com relação à confidencialidade, ou não, de determinada informação, este deverá consultar a área responsável pela gestão da segurança da informação.

REGISTROS DE OPERAÇÕES E INFORMAÇÕES FINANCEIRAS E CONTÁBEIS
Registros das diversas operações e atividades desenvolvidas pela SCC CHECK devem ser criados e relatados com integridade e precisão. Todos são responsáveis ou co-responsáveis pela integridade da informação e dos registros da empresa, sejam operacionais, comerciais, financeiros, contábeis ou administrativos. Os relatos e registros (em papel ou eletrônicos) devem estar em conformidade com as normas geralmente aceitas e praticadas pelas empresas privadas no País; e em conformidade com as normas e o sistema de controles internos da SCC CHECK.

Os registros e informações financeiras e contábeis devem ser mantidos e preservados de acordo com as leis e políticas aplicáveis relativas à guarda desses tipos de registros.
Qualquer registro potencialmente relevante para um caso de infração da lei, ou para qualquer litígio ou investigação pendente, não pode ser destruído.

RESPONSABILIDADES

Diretorias, gerências e coordenadorias:

- Conduzir-se eticamente perante os membros de sua equipe;
- Cumprir e fazer cumprir este Código de Conduta;
- Divulgar este Código de Conduta a sua equipe e certificar-se de sua leitura e compreensão;
- Orientar os profissionais sob sua responsabilidade acerca de ações ou situações que representem eventuais dúvidas ou dilemas de natureza ética;
- Comunicar eventuais casos de descumprimento deste Código de Conduta ao seu superior hierárquico imediato;
- Encaminhar os Termos de Compromisso, devidamente preenchidos e assinados pelos profissionais, à Gerência de Recursos Humanos, em que serão arquivados nos prontuários de cada Colaborador.

Todos os demais Colaboradores:

- Adotar comportamento e postura ética, em conformidade com os preceitos deste Código de Conduta;
- Cumprir este Código de Conduta;
- Buscar orientação do superior imediato para eventuais situações ou dilemas de natureza ética;
- Comunicar ao superior imediato os fatos que conheça e que representem conduta ilegal, duvidosa e não-ética, caracterizando possíveis violações a este Código de Conduta.

CUMPRIMENTO DO CÓDIGO

O desrespeito a este Código de Conduta levará à abertura de sindicância administrativa para averiguação de possíveis irregularidades e poderá sujeitar os Colaboradores a medidas disciplinares, inclusive demissão por justa causa e demais penalidades previstas na legislação trabalhista, independentemente de outras ações que a SCC CHECK possa adotar.
As disposições acerca do dever de confidencialidade estipulado neste CÓDIGO permanecerão validas por até 2 (dois) anos contados a partir do desligamento de Colaborador, por qualquer motivo, mantendo-se as PARTES obrigadas a respeitar todas as condições dispostas no presente instrumento, exceto se, por conveniência, a SCC CHECK dispuser de forma diversa no acordo de que trata.
Os Colaboradores que deliberadamente deixarem de notificar violações a este Código de Conduta ou omitirem informações relevantes também estarão sujeitos a medidas disciplinares.
Os casos que não estejam nele explicitados serão tratados como exceção e encaminhados A Diretoria da SCC CHECK, que analisará e decidirá conforme os princípios deste Código.

PROCESSAMENTO DAS DENÚNCIAS

As denúncias deverão ser encaminhadas por escrito para qualquer um dos membros da Diretoria da SCC CHECK não sendo admitidas denúncias anônimas.
A Diretoria garantirá se solicitado, o sigilo do denunciante.

ENTRADA EM VIGOR

Este Código esta em vigor, sendo revogadas todas e quaisquer disposições em contrário, inclusive aquelas que constam do contrato de trabalho firmado com a SCC CHECK.

Ao ler esta Política de Privacidade o leitor declara ter feita a completa e atenta leitura das regras.

Caso você ainda tenha dúvidas, reclamações ou queira se comunicar com a SCC Check a respeito da Política de Segurança, práticas e conduta, você pode entrar em contato conosco através do e-mail: sgo@scccheck.com.br

Em caso de dúvidas referentes à produtos ou serviços contratados, favor entrar no portal e clicar em nosso bot de atendimento lá você será direcionado para o setor que precisa

Atualizado em 07/06/2023.

SCC SISTEMA DE CONSULTA DE CRÉDITO LTDA
SCC CHECK