Programa de Integridade
do Grupo SEK - Security Ecosystem Knowledge

POLÍTICA ANTICORRUPÇÃO E ANTISSUBORNO

SEK Security Ecosystem Knowledge

Olá!

Somos parte de um Grupo que atua, dentre outras atividades, com o desafio de atender inúmeros clientes todos os dias. Em nossos negócios, nos relacionamos com nossos clientes, colegas de trabalho, vários parceiros comerciais, com a comunidade onde atuamos e com a administração pública em todas as esferas.

A Política Anticorrupção e Antissuborno ("Política") que ora apresentamos para vocês reforça o nosso compromisso com esses princípios e valores.

O Grupo SEK – Security Ecosystem Knowledge não admite nenhuma prática de corrupção ou suborno adotando uma política de "tolerância-zero" frente a qualquer ação ou omissão que possa repercutir em violação às disposições legais a respeito, sendo assim espera a cooperação de seus Colaboradores e todos que com ele se relacione à observância integral da legislação e desta Política.

Contamos com você para a leitura dessa Política e incentivamos a denúncia de quaisquer atos repudiados neste documento!

Presidente – Grupo SEK – Security Ecosystem Knowledge

SUMÁRIO

1. OBJETIVO:

1.1. A presente Política Anticorrupção e Antissuborno ("Política"), conforme aprovada pelo Conselho de Administração tem como objetivo estabelecer as diretrizes, padrões e procedimentos do programa de prevenção e combate à corrupção para todas as empresas do grupo econômico do qual é parte, em consonância à legislação vigente, Código de Conduta e Ética do Grupo SEK - Security Ecosystem Knowledge, políticas, manuais, instruções de trabalho e procedimentos estabelecidos por cada empresa do referido grupo.

2. DEFINIÇÕES:

2.1. Quando grafadas com a primeira letra maiúscula, são atribuídos os seguintes significados para as expressões a seguir:

"Administração Pública": é qualquer órgão ou entidade da administração pública direta ou indireta, nacional ou estrangeira, que desempenhe atividades de gestão e/ou execução de serviços públicos, nas esferas federal, estadual ou municipal.

"Administrator(es)": Significa, quando referidos no singular ou plural, os diretores estatutários e os membros do Conselho de Administração do Grupo SEK - Security Ecosystem Knowledge.

"Agente(s) Público(s)": Toda pessoa que: (i) ainda que transitoriamente ou sem remuneração, exerça cargo, emprego ou função pública em qualquer órgão ou entidade da Administração Pública ou em empresa contratada ou conveniada para a execução de atividade objeto de concessão pela Administração Pública; (ii) exerça cargo, emprego ou função em empresas públicas ou controladas pelo governo, incluindo sociedades de economia mista, bem como em fundações públicas; (iii) integra partido político ou é candidata a cargo político; e (iv) exerça cargo, emprego ou função pública em órgãos, entidades estatais ou em representações diplomáticas de país estrangeiro, assim como em pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro ou em organizações públicas internacionais. A definição de Agente Público inclui pessoas politicamente expostas (PEP), que podem ser definidas como pessoas que ocupam ou tenham ocupado cargos, empregos ou funções públicas relevantes.

"Canal de Transparência": É aquele previsto no item 12 deste documento, que tem como finalidade servir de instrumento para que Colaboradores e Terceiros possam comunicar suas preocupações e denúncias relacionadas a esta Política, bem como solicitar o esclarecimento de dúvidas.

"Colaboradores": Significa o público interno das empresas do Grupo SEK - Security Ecosystem Knowledge, ou seja, no plural ou singular, todo(s) o(s) empregado(s), Administrador(es), estagiário(s), aprendizes(s), membro(s) de comitês de governança corporativa, considerando todos os segmentos de negócios, bem como suas divisões e marcas de atuação.

"Corrupção": É oferecer, prometer, dar ou receber, direta ou indiretamente, alguma coisa a alguém com o objetivo de influenciar a tomada de decisão de forma a obter uma Vantagem Indevida. A simples promessa, sem a efetiva entrega de "alguma coisa", é também considerada ato de corrupção. O bem

oferecido, recebido ou prometido não se limita a valores em espécie. Pode ser também qualquer benefício ou favor, incluindo pagamento de despesas, oferta de presentes, viagens, entretenimentos, entre outras condutas.

"Grupo SEK – Security Ecosystem Knowledge": Significa a CBS HOLDING GLOBAL, LTD. e todas as demais empresas por esta controladas e/ou coligadas, que sejam pertencentes ou venham a integrar o mesmo grupo econômico do qual faz parte.

"Lei Anticorrupção e Antissuborno": Significa todas as leis e regulamentações nacionais ou estrangeiras aplicáveis visando estabelecer regras que irão coibir as práticas de corrupção, suborno, improbidade administrativa, violação de licitações e contratos públicos, lavagem de dinheiro, doações políticas ou eleitorais, incluindo, sem limitação a Lei de Combate à Corrupção Brasileira (Lei 12.846/13) regulamentada pelo Decreto 8.420/15 e respectivas alterações, Decreto-Lei nº 2.848/1940 (Código Penal Brasileiro); Lei nº 8.429/1992 (Lei de Improbidade Administrativa Brasileira); Lei nº 8.666/1993 (Lei de Licitações Brasileira); Lei nº 9.504/1997 (Lei Eleitoral Brasileira); Lei nº 9.613/1998 (Lei de Prevenção à Lavagem de Dinheiro Brasileira); Lei de Práticas de Corrupção no Exterior (FCPA); e U.K. Bribery Act (UKBA), incluindo seus regulamentos e outras regras relacionadas, bem como suas futuras alterações

"Pessoa(s) Relacionada(s)": Pessoas relacionadas a um Agente Público por qualquer razão, incluindo, sem limitação, membros da família ou parentes de Agente Público, tais como cônjuge, companheiro(a), irmãos, pais, filhos ou enteados, avós, netos, genros, noras, tios, sobrinhos, cunhados e sogros.

"Política": A presente Política Anticorrupção e Antissuborno.

"Terceiros": Significa todo o público externo do Grupo SEK - Security Ecosystem Knowledge, ou seja, aquele sem vínculo empregatício ou estatutário, tais como os fornecedores de bens e/ou serviços, clientes, procuradores, consultores em geral e demais terceiros que mantenham ou pretendam manter relacionamento com as empresas integrantes do Grupo SEK - Security Ecosystem Knowledge, sob qualquer natureza e forma, bem como quaisquer pessoas físicas e/ou jurídicas subcontratadas e/ou vinculadas aos mesmos.

"Vantagem Indevida": é todo evento, com valor econômico ou não, que não teria ocorrido não fosse pela promessa ou oferta de "alguma coisa" ou "algum bem". A celebração de um contrato ou a dispensa do pagamento de uma penalidade são exemplos de vantagem indevida, assim como acesso a informações confidenciais e privilegiadas. O termo vantagem indevida deve ser interpretado em sentido amplo, por qualquer natureza e forma

3. APLICABILIDADE:

3.1. Esta Política aplica-se a todas as empresas integrantes do Grupo SEK - Security Ecosystem Knowledge e, indistintamente e indiscriminadamente, a todos os Colaboradores e Terceiros que com elas se relacionem, de forma isenta e imparcial, dentro do compromisso do Grupo SEK - Security Ecosystem Knowledge em conduzir seus negócios com ética, integridade e em consonância com a legislação vigente nos países nos quais o Grupo SEK - Security Ecosystem Knowledge atua ou esteja submetido.

4. VIGÊNCIA, ALTERAÇÕES E ATUALIZAÇÕES:

4.1. A presente Política tem vigência por prazo indeterminado, sendo que atualizações e alterações poderão ser realizadas conforme aprovadas pelo Conselho de Administração.

5. COMENTÁRIOS INICIAIS E PREMISSAS:

5.1. O compromisso com a ética e a integridade deve determinar e guiar todas as ações dos Colaboradores, Terceiros e relacionamentos do Grupo SEK - Security Ecosystem Knowledge, na condução de seus negócios e atividades, sempre em conformidade com os mais elevados padrões morais e legais, não tolerando qualquer forma de Corrupção, suborno pagamento de facilitação, favorecimentos indevidos ou quaisquer outras condutas impróprias, independentemente do valor envolvido.

5.2. A SEK e todos aqueles que com ele se relacionem, interna ou externamente, devem entender e agir em conformidade com as leis de combate à corrupção e suborno aplicáveis, em todas as relações com a Administração Pública e Agentes Públicos.

5.3. Violações às leis de combate à corrupção e suborno não são toleradas, bem como podem expor o Grupo SEK - Security Ecosystem Knowledge , seus acionistas, Administradores e Colaboradores, às consequências gravosas quanto a reputação e imagem, além de possíveis penalidades administrativas, judiciais e criminais.

5.4. É de responsabilidade do Grupo SEK - Security Ecosystem Knowledge, todos os seus Colaboradores e Terceiros, conhecer, disseminar e cumprir todos os termos desta Política.

5.5. As Leis Antissuborno e Anticorrupção não penalizam somente o indivíduo que comete o ato de Corrupção, mas também os indivíduos que agiram de maneira a incentivá-lo, ou seja, se aplicam a qualquer indivíduo que:

- Aprove o pagamento de propina ou qualquer tipo de Vantagem Indevida;
- Forneça ou aceite faturas emitidas de maneira fraudulenta;
- Retransmita instruções para pagamento de Propina ou de qualquer tipo de Vantagem Indevida;
- Encubra o pagamento de Propina ou realização de Vantagem Indevida; ou
- Coopere com ato de Corrupção.

5.6. Caso haja qualquer dúvida sobre o teor dessa Política e sua aplicação, solicitar esclarecimentos ao Comitê de Ética através do Canal de Transparência (indicado no item 12 abaixo).

6. DIRETRIZES E REGRAS:

6.1. O Grupo SEK – Security Ecosystem Knowledge está comprometida em conduzir suas atividades em estrito cumprimento às leis aplicáveis, incluindo legislações Anticorrupção e Antissuborno e demais normas que regem o relacionamento com a Administração Pública e Agentes Públicos.

6.2. Pagamentos Indevidos a Agentes Públicos: é estritamente proibido prometer, oferecer ou dar, direta ou indiretamente, qualquer Vantagem Indevida a Agentes Públicos nacionais ou estrangeiros ou a Pessoas Relacionadas.

6.2.1. A proibição prevista nesta Política se aplica tanto às condutas cometidas diretamente por quaisquer das empresas do Grupo SEK - Security Ecosystem Knowledge ou aquelas cometidas por seus Colaboradores e/ou Terceiros.

6.2.2. A proibição expressa contida nesta Política também se aplica a pagamentos que tenham como objetivo acelerar ou agilizar a prática de atos rotineiros por parte de Agentes Públicos (e.g., emissão de licenças, alvarás ou autorizações; certidões, realização de inspeções ou visitas) (conhecidos como pagamentos ou taxas de "agilização", "aceleração" ou "urgência"). Tais pagamentos são expressamente proibidos por esta Política e não poderão ser feitos, em hipótese alguma, seja diretamente ou através de quaisquer Terceiros e/ou em qualquer valor ou forma.

6.3. Pagamentos Indevidos a Particulares: é estritamente proibido oferecer ou autorizar, direta ou indiretamente, qualquer oferta, promessa de pagamento ou pagamento por meio de Vantagem Indevida, a qualquer empregado, agente ou representante de empresa privada que tenha (ou possa vir a ter) relacionamento comercial com as empresas do Grupo SEK - Security Ecosystem Knowledge e que possa representar qualquer conflito de interesses ou para fins de tentar obter interesses indevidos com estas empresas ou, indiretamente, com ou envolvendo empresas públicas.

6.4. Pagamentos Indevidos à Administradores, Colaboradores ou Terceiros: esta Política também se aplica à oferta de Vantagens Indevidas à Colaboradores e Terceiros. É estritamente proibido para qualquer Colaborador e Terceiro solicitar, oferecer, prometer, receber ou aceitar qualquer Vantagem Indevida, de qualquer terceiro, em benefício próprio ou de pessoa relacionada, de modo a influenciar a prática de qualquer ato no desempenho de suas atividades nas e para as empresas do Grupo SEK – Security Ecosystem Knowledge.

6.5. Respostas às Solicitações ou Demandas de Pagamentos Indevidos: caso você receba uma solicitação de pagamento extraordinário ou de qualquer Vantagem Indevida por parte de Agente Público ou Pessoa Relacionada, recuse imediatamente, de forma explícita e definitiva, e avise com a máxima urgência seu superior imediato ou o Comitê de Ética (através do Canal de Transparência disponível conforme indicado no item 12 abaixo).

6.6. Relacionamento com Agentes Públicos: o relacionamento com Agentes Públicos deve ser pautado nas diretrizes desta Política, no respeito, na legalidade, com ética e transparência. Os Colaboradores poderão manter contato com Agentes Públicos tão somente quando necessário em razão de suas atribuições corporativas, e nas instalações dos órgãos públicos e/ou nas instalações de empresas do Grupo SEK - Security Ecosystem Knowledge, neste último caso, sempre na presença de dois ou mais Colaboradores. Essa regra deverá ser observada também por Terceiros conforme aplicável.

6.6.1. Reuniões: a realização de reuniões com Agentes Públicos:

- Deve ser precedida de solicitação formal por escrito, protocolada no órgão correspondente, por meio eletrônico ou fax, quando possível. A solicitação deverá conter a identificação do requerente; a data e hora em que pretende ser ouvido e, quando for o caso, as razões da urgência; o assunto a ser abordado; e a identificação de acompanhantes, se houver, e seu interesse no assunto;
- Devem ser realizadas em órgão, repartições ou edifícios públicos apropriados, em horário comercial, ou durante plantões devidamente previstos nas normas de funcionamento dos órgãos.
- Devem contar, preferencialmente, com a presença de dois representantes das empresas do Grupo SEK - Security Ecosystem Knowledge;
- Devem ser registradas na agenda corporativa (Outlook).
- Registros em calendários digitais (ex.: Outlook) obrigatoriamente devem ter back-up, para proteção da informação sobre a ocorrência da reunião;
- Após a reunião, devem ser devidamente registradas, com a indicação dos nomes de todos os participantes, data, horário e local da reunião, bem como breve resumo dos assuntos abordados e quaisquer outras informações relevantes;
- No caso de acompanhamento de Agentes Públicos em fiscalizações e visitas *in loco*, os Colaboradores, Administradores e Terceiros devem somente prestar informações exclusivamente técnicas e operacionais apresentando apenas os documentos exigidos pela autoridade; e
- Procedimentos para obtenção e renovação de licenças, permissões e autorizações governamentais devem seguir um procedimento claro e transparente e deverão ser efetuados por pessoas treinadas, sendo expressamente proibido o pagamento de qualquer taxa, a qualquer título, não prevista em leis e regulamentos aplicáveis, devendo todos os questionamentos serem respondidos de forma oficial e com argumentos técnicos e jurídicos.

6.6.2. Mensagens de e-mail e ligações telefônicas:

- Devem ter conteúdo claro e objetivo e devem sempre ter como destinatários ao menos 2 (dois) Colaboradores do Grupo SEK - Security Ecosystem Knowledge;
- Devem ter linguagem técnica, respeitosa, cordial e adequada; e
- Quando forem tratados assuntos estratégicos em ligações telefônicas, recomenda-se que o conteúdo da conversa seja posteriormente registrado por escrito e direcionado a todos aqueles que estiverem envolvidos no assunto, inclusive aqueles que não tenham participado da ligação.

6.6.3. Melhores Práticas de Interação com Agentes Públicos:

- O relacionamento com Agentes Públicos deve ser ético, profissional, cordial e transparente, com comunicação técnica, clara e direta, evitando-se interpretações dúbias;
- Ao encontrar Agentes Públicos em ocasiões sociais, evitar o contato e, se não for possível, manter grau de profissionalismo e formalidade adequados, não tratando em hipótese alguma de assuntos sensíveis do Grupo SEK - Security Ecosystem Knowledge fora dos ambientes próprios;
- Sempre evitar interações com Agentes Públicos que possam parecer suspeitas ou sugerir a prática de irregularidades (encontros em

estacionamentos, quartos de hotéis, envio de mensagens codificadas, entre outros); e
- No caso de interações informais com Agentes Públicos (seminários, associações, conferências, aniversários, festas, jantares, entre outros), os Administradores, Colaboradores e Terceiros devem se abster de tratar assuntos específicos e de interesse do Grupo SEK - Security Ecosystem Knowledge. Se o Agente Público tomar a iniciativa de abordar o assunto, deverá ser sugerida a realização de uma reunião específica, em ambiente profissional e horário comercial, para manter o caráter profissional e institucional da interação.

6.7. Brindes e Entretenimento: tanto a oferta quanto o recebimento de brindes, hospitalidade e entretenimento devem observar as seguintes regras, limites e procedimentos:

- NÃO poderão ser realizadas OFERTAS, RECEBIMENTO, CONCESSÃO ou PROMESSA de qualquer Vantagem Indevida, incluindo brindes, hospitalidade, entretenimento ou quaisquer outras vantagens que envolvam Agentes Públicos, independentemente do valor ou tipo de vantagem/benefício. Quando NÃO envolvam Agentes Públicos, deverão ser observadas as regras estabelecidas no Código de Conduta e Ética do Grupo SEK - Security Ecosystem Knowledge;
- NÃO é permitido receber e manter PRESENTES, BRINDES, HOSPITALIDADE ou ENTRETENIMENTO fora do permitido em lei e dos critérios estabelecidos nesta Política. Caso o Colaborador ou Terceiro, atuando em nome de quaisquer empresas do Grupo SEK - Security Ecosystem Knowledge receba brinde em desacordo com esta Política, deverá providenciar a devolução do brinde ao remetente, com uma carta padrão de agradecimento, conforme previsto no Código de Conduta e Ética do Grupo SEK - Security Ecosystem Knowledge;
- A realização e participação em eventos específicos e que envolvam a Administração Pública e Agentes Públicos deverá estar alinhada com os preceitos legais, éticos e com os interesses do Grupo SEK - Security Ecosystem Knowledge, bem como será possível apenas mediante aprovação prévia do Comitê de Ética; e
- Se houver qualquer dúvida se um brinde ou entretenimento é apropriado ou permitido, consulte o Comitê de Ética (através do Canal de Transparência previsto no item 12 abaixo).

6.8. Relacionamento com Órgãos Reguladores: o relacionamento com profissionais de Órgãos Reguladores, dentre outros, deve ser pautado nos mais elevados padrões morais e éticos, observado o disposto na legislação vigente, no Código de Conduta e Ética do Grupo SEK - Security Ecosystem Knowledge e nesta Política.

6.9. Participação no Processo Político: o Grupo SEK – Security Ecosystem Knowledgenão participa do processo político, porém, respeita o direito individual de cada um de seus Colaboradores e Terceiros de participarem do processo político no país em que residem, porém, quando isto ocorrer, referida participação deverá ser posicionada como de caráter individual, sendo expressamente proibido usar o nome, logotipos, marcas e quaisquer sinais distintivos do Grupo SEK - Security Ecosystem Knowledge ou dar a impressão de estar agindo em nome deste. Nenhuma campanha política, de

qualquer tipo, está permitida nas instalações das empresas do Grupo SEK - Security Ecosystem Knowledge, tais como distribuição de panfletos, envio e-mails corporativos, registros nos chats de trabalho, dentre outros.

6.10. Patrocínios: é vedado quaisquer patrocínios a qualquer pessoa física ou jurídica, Agente Público ou não, com o objetivo de influenciar, direta ou indiretamente uma decisão de negócios. O patrocínio, quando autorizado pelas alçadas competentes, deve observar um processo formal de contratação, ou seja, para que seja realizado deve ser previamente informado ao Departamento Jurídico do Grupo SEK - Security Ecosystem Knowledge, com informações detalhadas, e ser autorizado previamente pelo Comitê de Ética. O patrocínio deverá ser baseado em instrumentos contratuais formalizado entre a empresa do Grupo SEK - Security Ecosystem Knowledge e Terceiros que receberão o mesmo, bem como registrados contabilmente de forma adequada transparente.

6.11. Doações Políticas e Contribuições de Caridade: a legislação pode permitir em determinadas situações as doações e contribuições políticas por pessoas físicas dentro dos limites e procedimentos legais, sendo que tal fato, quando legalmente permitido, é respeitado pelo Grupo SEK – Security Ecosystem Knowledge desde que seja realizado em caráter estritamente pessoal e sem qualquer vinculação com as empresas do grupo. É' terminantemente proibido fazer doações políticas para candidatos a cargos políticos ou a partidos políticos através das empresas do Grupo SEK - Security Ecosystem Knowledge ou em nome destas.

6.11.1. Contribuições de caridade podem ser feitas apenas mediante o integral atendimento da legislação vigente, do Código de Conduta e Ética do Grupo SEK - Security Ecosystem Knowledge, seguindo as diretrizes desta Política e desde que aprovada previamente pelo Comitê de Ética. Se legalmente permitidas e devidamente aprovadas, eventuais contribuições de caridade somente poderão ser feitas por empresas do Grupo SEK - Security Ecosystem Knowledge (e não diretamente e em nome de qualquer Colaborador), devendo serem registradas e contabilizadas adequadamente e de forma transparente, observados os limites e as formalidades da legislação aplicável. Nesse sentido, Colaboradores devem assegurar ainda que contribuições de caridade eventualmente realizadas pelo Grupo SEK – Security Ecosystem Knowledge conforme autorizadas, sejam sempre utilizadas pelas instituições beneficiárias somente para fins de caridade e que não sejam aplicadas de forma errônea, política ou violando esta Política ou quaisquer outros preceitos éticos e leis aplicáveis.

6.12. Controles Contábeis: é responsabilidade de todos os Colaboradores garantir a manutenção de registros contábeis de forma precisa, correta e completa, de todas as despesas, transações e pagamentos das empresas do Grupo SEK - Security Ecosystem Knowledge. É estritamente proibido fazer registros falsos ou imprecisos, que ocultem a natureza ou o valor correto de qualquer operação. Nenhum fundo ou conta não oficial ou sem registro poderão ser criados ou mantidos para nenhum fim e sob qualquer justificativa, e nenhum lançamento falso, enganoso ou impreciso poderá ser

feito nos livros e registros contábeis do Grupo SEK - Security Ecosystem Knowledge.

6.13. Contratação de Terceiros: o Grupo SEK – Security Ecosystem Knowledge se preocupa em fazer negócios apenas com Terceiros que sejam conceituados, idôneos e que compartilhem seus princípios éticos, inclusive no que se refere à não tolerância a qualquer forma de corrupção e suborno. Em certas circunstâncias, as ações de Terceiros podem gerar responsabilidade direta as empresas do Grupo SEK - Security Ecosystem Knowledge, por essa razão é essencial realizar uma análise de risco adequada e seguir procedimentos e precauções ao contratar e/ou nomear Terceiros para prestarem serviços e/ou agir em nome de quaisquer das empresas do Grupo SEK - Security Ecosystem Knowledge, em seu interesse ou de seus Colaboradores.

6.13.1. Pré-Contratação: Antes de fazerem negócios com o Grupo SEK – Security Ecosystem Knowledge, todos os Terceiros deverão passar por uma análise que verificará especialmente, mas não se limitando, ao relacionamento com Agentes Públicos, Administração Pública e Pessoas Relacionadas, reputação e qualificações para executarem o trabalho para o qual seriam contratados.

- Esta análise deve ser providenciada pelo responsável pela contratação, o qual deverá envolver os demais departamentos que devam assessorá-lo no assunto, especialmente a área jurídica e de compras. Adicionalmente, o responsável interno pela contratação deve manter a análise em arquivo para disponibilização sempre que solicitado pela Administração, pelo Comitê de Ética ou área jurídica;

- O processo de análise será composto por uma revisão a ser feita de maneira independente pelo Colaborador responsável pela contratação, sendo que o Terceiro deverá cooperar e disponibilizar todas as informações que lhe forem solicitadas sob pena de não contratação. Todo processo de contratação deve ser feito com base no mérito e não mediante o uso indevido de influência sobre qualquer pessoa, seja Agente Público ou não.

- Os contratos celebrados pelo Grupo SEK – Security Ecosystem Knowledge com Terceiros, deverão conter a descrição clara do respectivo objeto contratado, valores em conformidade com os preços de mercado, vigência, obrigações das partes contratantes e, entre outras questões que entenderem necessárias, deverão obrigatoriamente conter as cláusulas de cumprimento desta Política e, quando aplicável, deverão observar o procedimento de *Due Diligence* de Terceiros de acordo com as regras do Grupo SEK - Security Ecosystem Knowledge.

6.13.2. Pós- Contratação: após a contratação dos Terceiros, é dever do gestor responsável pela contratação acompanhar suas atividades, sempre atento a eventuais sinais de alerta ou de descumprimento às Leis Antissuborno e Anticorrupção e reportar qualquer sinal de preocupação conforme previsto no item 12 desta Política. Caso o Colaborador não seja o gestor responsável pela contratação, mas saiba ou tenha motivo legítimo para crer que um pagamento

proibido pelas Leis Antissuborno e Anticorrupção ou por esta Política tenha sido, esteja sendo ou possa ser feito ou prometido a um Terceiro ou Agente Público em nome das empresas do Grupo SEK - Security Ecosystem Knowledge, direta ou indiretamente, este deve comunicar tal fato imediatamente aos canais de comunicação mencionados no item 12 abaixo.

6.14. Contratos com a Administração Pública – Licitações, pregões, concessões, etc.: a contratação com a Administração Pública segue padrões e procedimentos previstos em legislação específica que são muito diferentes daqueles aplicáveis aos contratos firmados com a iniciativa privada. Por essa razão os Colaboradores e Terceiros devem ficar atentos ao disposto na legislação específica sobre esse tipo de contratação, incluindo sempre a área jurídica no processo de análise de participação da contratação e análise prévia da documentação pertinente para sua celebração.

6.14.1. Todos os envolvidos no processo de contratação com a Administração Pública devem agir de acordo com os mais altos padrões éticos e dentro da lei ao interagirem com Agentes Públicos e com competidores, respeitando a legislação aplicável, esta Política e procedimentos internos estabelecidos para esse tipo de contratação.

6.14.2. É terminantemente proibido praticar, direta ou indiretamente, qualquer ato que possa ser entendido como fraude, lesão ou frustração de processos seletivos realizados pela Administração e Agentes Públicos.

6.14.3 Caso haja qualquer dúvida sobre como se relacionar com a Administração Pública, Agentes Públicos, órgãos governamentais ou competidores em um contexto de licitações ou contratos públicos, encaminhe consulta ao Comitê de Ética (através do Canal de Transparência indicado no item 12 abaixo).

7. OPERAÇÕES DE FUSÕES, AQUISIÇÕES E INCORPORAÇÕES:

7.1. Todas as vezes em que o Grupo SEK – Security Ecosystem Knowledge buscar novos negócios através de aquisição, fusão ou incorporação de qualquer empresa ou ativo, deve ser realizado um processo de *Due Diligence* criterioso e incluído no contrato de compra e venda as cláusulas anticorrupção adequadas, bem como consideradas outras opções disponíveis para evitar o risco de sucessão de qualquer passivo anterior ao fechamento da operação.

7.2. Deve ser realizado, no processo de *Due Diligence*, um procedimento para fins de verificação do cumprimento das disposições das Leis Antissuborno e Anticorrupção previamente à realização do negócio. Caso sejam identificadas quaisquer violações ou suspeitas de violações às Leis Antissuborno e Anticorrupção, a área de Jurídica e de Compliance do Grupo SEK - Security Ecosystem Knowledge deverá ser comunicado formalmente para as providências cabíveis ao atendimento do Programa de Integridade e desta Política.

8. COMPROMISSO DE REPORTAR:

8.1. É responsabilidade de todos os Colaboradores e Terceiros, comunicar qualquer violação, comportamentos incompatíveis ou suspeita de violação aos princípios da ética, honestidade, comprometimento, responsabilidade e seriedade, ao Código de Conduta e Ética do Grupo SEK - Security Ecosystem

Knowledge, leis e regulamentos em vigor, desta Política, bem como das demais políticas, manuais e procedimentos internos.

8.2. As violações ou suspeitas devem ser comunicadas ao Canal de Transparência (vide item 12 abaixo), podendo ser feita de forma identificada ou anônima.

8.3. Não será tolerada retaliação ou represália em qualquer formato ou medida, contra qualquer Colaborador ou Terceiro que venha apresentar uma denúncia de boa fé.

8.4. Quando da comunicação das violações, deverá ocorrer a pronta interrupção de irregularidades ou infrações detectadas, cabendo ao Comitê de Ética do Grupo SEK - Security Ecosystem Knowledge auxílio para a tratativa e remediação dos danos gerados.

9. RESPONSABILIDADES:

9.1. É de responsabilidade de todos os Colaboradores a disseminação da presente Política, bem como zelar pelo cumprimento do Código de Conduta e Ética do Grupo SEK - Security Ecosystem Knowledge, fazendo com que quaisquer Terceiros também estejam comprometidos com referidos documentos.

9.2. O Grupo SEK – Security Ecosystem Knowledgepromoverá periodicamente treinamentos relacionados ao seu Programa de Integridade, os quais poderão ser presenciais ou na modalidade à distância, devendo os Colaboradores e Terceiros participarem dos mesmos para o fim de garantir o cumprimento de suas responsabilidades definidas no item 9.1 desta Cláusula.

10. VIOLAÇÕES E PENALIDADES:

10.1. Violações a esta Política também serão consideradas como infrações ao Código de Conduta e Ética do Grupo SEK - Security Ecosystem Knowledge, sujeitando seus infratores às penalidades legais conforme aplicáveis e nos termos da Política de Gestão de Consequências do Grupo SEK - Security Ecosystem Knowledge.

10.2. Os Terceiros responderão civilmente e criminalmente por infrações a esta Política, além da aplicação das penalidades contratuais previstas, incluindo perdas e danos cabíveis e observados os termos contratuais e, ainda, da Política de Gestão de Consequências do Grupo SEK - Security Ecosystem Knowledge.

10.3. A omissão, diante do conhecimento de possíveis violações por Colaboradores e Terceiros, será considerada atitude antiética e passível de aplicação de medidas disciplinares. Da mesma forma, o relato de situações irreais com o objetivo de prejudicar outras pessoas ou empresas por interesses pessoais ou escusos será igualmente considerado antiético e passível de penalidades, nos termos desta Política.

11. CONFLITOS, EXCEÇÕES E ESCLARECIMENTOS:

11.1. Qualquer exceção ao determinado nesta Política deverá ser requerida mediante o envio de solicitação endereçada ao Comitê de Ética (através do Canal de Transparência indicado no item 12 abaixo) do Grupo SEK - Security Ecosystem Knowledge, com a descrição do requerimento, justificativas e critérios utilizados para o pedido, utilizando-se para tanto do formulário modelo que segue no Anexo I da presente Política.

11.2. Nenhuma exceção poderá ser realizada antes de devidamente aprovada pelo Comitê de Ética, tampouco em desacordo com a legislação vigente e com as diretrizes e premissas do Programa de Integridade.

12. CANAL DE TRANSPARÊNCIA:

12.1. O Grupo SEK – Security Ecosystem Knowledge incentiva todos os seus Colaboradores e Terceiros a denunciarem quando suspeitarem ou detectarem violações.

12.2. Todos que se relacionam com a SEK devem comunicar as violações ou possíveis violações às diretrizes desta Políticas e demais regras estabelecidas pelo Programa de Integridade dele, por meio do Canal de Transparência, que está acessível em: https://canaldatransparencia.com.br/sek-securityecosystemknowledge/

12.3. Os relatos podem ser realizados pelo denunciante de forma anônima, caso este prefira não se identificar. Todas as situações reportadas serão avaliadas e as devidas tratativas conduzidas pelo Comitê de Ética do Grupo SEK - Security Ecosystem Knowledge dentro do mais estrito sigilo, com justiça, profundidade, tempestividade, respeito e razoabilidade.

Toda denúncia poderá ser feita de maneira anônima.
É assegurado o sigilo para todas as pessoas e situações relatadas.

***

Anexo I

FORMULÁRIO PARA SOLICITAÇÃO DE EXCEÇÃO À DISPOSIÇÃO ESPECÍFICA RELACIONADA À POLÍTICA ANTICORRUPÇÃO E ANTISSUBORNO

Ao Comitê de Ética do Grupo SEK - Security Ecosystem Knowledge,

Solicitante: [inserir]

Venho pelo presente solicitar exceção à seguinte disposição específica relacionada à Política Anticorrupção e Antissuborno do Grupo SEK - Security Ecosystem Knowledge:

- [inserir]

Tal solicitação de exceção específica está relacionada à:

- Data: [inserir]
- Participantes Grupo SEK – Security Ecosystem Knowledge: [inserir]
- Participantes da outra Parte: [inserir]
- Local: [inserir]
- Valor: [inserir]
- Departamento: [inserir]
- Relação com a outra parte: [inserir]
- Finalidade: [inserir]

A solicitação de exceção se justifica [inserir justificativa para o pedido de exceção específica].

Por este ato DECLARO que todas as informações acima prestadas são corretas, completas e verdadeiras e reconheço que a prestação de informações incorretas ou sua omissão podem resultar em penalidades legais e contratuais.

Adicionalmente, DECLARO que somente após a autorização formal do Comitê de Ética é que poderei seguir com a eventual implementação da exceção, se aprovada.

Fico no aguardo de vossa deliberação para continuidade ao assunto.

[Local], [●] de [●] de [●].

_____

Nome Completo
Assinatura