POL-002 Política de Segurança da Informação

Sumário

1. Objetivo

Esta política tem como objetivo:

- Estabelecer diretrizes que permitam aos Funcionários e Terceiros da Companhia observarem os padrões de comportamento relacionados à Segurança da Informação adequados às necessidades de negócio, de proteção legal da Companhia e do indivíduo;

- Nortear a definição de normas e procedimentos específicos de Segurança da Informação e orientar as condições de uso dos Recursos de Tecnologia da Informação, bem como a implementação de controles e processos para seu atendimento; e

- Preservar as Informações da Companhia quanto à:

  - Integridade: garantia de que a Informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

  - Confidencialidade: garantia de que o acesso à Informação seja obtido somente por pessoas autorizadas;

  - Disponibilidade: garantia de que os Usuários autorizados obtenham acesso à Informação e aos ativos correspondentes sempre que necessário; e

  - Privacidade: garantia do Tratamento de Dados Pessoais em conformidade com a Lei Geral de Proteção de Dados (“LGPD”).

2. Âmbito de Aplicação

2.1 A presente política aplica-se a todos os Funcionários da BRK Ambiental Participações S.A. e de suas empresas controladas ou a ela afiliadas, cada qual doravante individualmente designada “Companhia”.

2.2 Da mesma maneira, a presente política abrange também todos os terceiros com os quais a Companhia mantenha ou venha a manter relações.

3. Considerações Gerais

3.1 O conteúdo desta política é propriedade da Companhia, destinado para uso e divulgação interna, e está disponível no portal da Companhia. Para garantir que seja sempre considerada a versão mais atualizada, não é recomendado que este documento seja reproduzido, armazenado ou transmitido, em qualquer formato ou por quaisquer meios, sejam eletrônicos ou físicos.

3.2 O conteúdo desta política deve ser conhecido e observado por todos os Funcionários e Terceiros, conforme abaixo definido, sendo o seu descumprimento passível de aplicação das medidas legais e disciplinares mencionadas no Código de Conduta Ética Profissional da Companhia.

3.3 Esta política dá ciência a cada Funcionário e Terceiro de que os ambientes, sistemas, computadores, notebooks, tablets, e-mails, internet, telefones fixos e

móveis, redes, CD, DVD, pendrive, HD Externo da Companhia ou dispositivos pessoais autorizados pela Área de TI poderão ser monitorados.

3.4 Os instrumentos normativos deverão ser interpretados como instrumentos dinâmicos, fonte constante de informação para a execução com excelência dos processos de trabalho da Companhia.

3.5 O cumprimento dos instrumentos normativos será objeto de auditoria periódica, visando o acompanhamento de sua utilização.

3.6 Em caso de dúvidas sobre a aplicação adequada das diretrizes constantes da presente política, os Funcionários e Terceiros devem consultar a Área de TI.

3.7 Os casos omissos serão decididos pela Comissão de Cibersegurança da Companhia.

4. Vínculos

Código de Conduta Ética Profissional
Código de Conduta Ética para Fornecedor
POL-010 Política de Privacidade e Proteção de Dados Pessoais
NOR-015 Norma de Segurança e Tecnologia da Informação
NOR-032 Norma de Resposta a Incidentes de Segurança da Informação

5. Conceitos

Os principais termos desta norma estão definidos no documento “Instrumentos Normativos – Glossário”, disponível na Plataforma de Compliance.

6. Diretrizes

6.1 Gerais

a) Toda Informação é de propriedade da Companhia, ressalvadas aquelas informações de propriedade de Terceiros que sejam obtidas pela Companhia através de um acordo de confidencialidade ou documento equivalente. São ativos corporativos valiosos que devem ser gerenciados com o devido cuidado.

b) Todos os Dados Pessoais e/ou Dados Pessoais Sensíveis devem ser protegidos contra o Tratamento não autorizado ou ilegal e de situações acidentais a fim de prevenir a ocorrência de Incidentes de Privacidade.

c) Os Dados Pessoais, Dados Pessoais Sensíveis e as Informações da Companhia devem ser usadas exclusivamente para fins empresariais.

d) Não é permitida a cópia e envio de Dados Pessoais, Dados Pessoais Sensíveis e Informações da Companhia sem autorização expressa do Responsável da Informação.

e) É responsabilidade de todos os Funcionários e Terceiros o descarte correto de mídias, devendo sempre utilizar fragmentador ou outro método para inutilizar

o acesso à Informações, aos Dados Pessoais e/ou Dados Pessoais Sensíveis nelas contidas.

f) Informações enviadas a Terceiros devem ser transportadas por portador autorizado e em envelope lacrado quando físicas ou através de dispositivo quando eletrônicas. Quando transmitidas por meios eletrônicos, o conteúdo deve ser protegido por senha (criptografia).

g) As diretrizes para envio de Dados Pessoais a terceiros estão definidas na POL-010 Política de Privacidade e Proteção de Dados Pessoais.

h) É dever de todos os Funcionários e Terceiros da Companhia:

- proteger e salvaguardar os ativos da Companhia de perda, roubo, mau uso e desperdício;
- proteger o sigilo das Informações, de acordo com a sua classificação, de propriedade da Companhia e Terceiros;
- tomar todas as medidas razoáveis para garantir a segurança de cópias impressas das Informações, de acordo com a sua classificação;
- ter discrição ao falar sobre assuntos envolvendo a Companhia em locais públicos, tais como elevadores, restaurantes, aviões ou ao utilizar qualquer dispositivo móvel fora do escritório.

i) Os Funcionários e Terceiros não podem transmitir Informações da Companhia para suas contas de e-mail pessoais nem salvá-las em seus computadores pessoais ou outros dispositivos eletrônicos que não sejam homologados pela Companhia.

j) As Informações, de acordo com a sua classificação, não podem ser deixadas em locais com acesso irrestrito, como diretórios públicos do servidor de arquivos da rede de dados e compartilhamento em nuvem, ou ainda como a mesa de trabalho, sala de recepção, copa e/ou salas de reunião da Companhia. Também deverá ser dispensada atenção no momento da impressão, envio e descarte dessas Informações.

k) Quanto ao envio de Informações, quer seja por fax, e-mail ou outras mídias, é necessário ter certeza que o destinatário pode ter acesso às Informações.

l) É imprescindível tomar os devidos cuidados com o manuseio, transmissão oral e escrita de Informações.

m) Cabe ao Gestor e ao Responsável da Informação tomar todos os cuidados para que Informações estejam acessíveis de acordo com a sua classificação e pela autorização do acesso dos Usuários à estas Informações, bem como a guarda em local restrito ou em base de dados eletrônica conforme recursos disponibilizados pela Área de TI para tal.

n) Não deve ser mantida nenhuma Informação, arquivo ou dado corporativo em discos locais ou qualquer outro meio de armazenamento senão aqueles disponibilizados ou homologados pela Área de TI.

o) Os Usuários de notebooks devem, preferencialmente, armazenar as Informações na rede de dados ou em Ambiente de Nuvem da Companhia, evitando o armazenamento em seus discos locais.

p) Todo incidente que coloque em risco a Segurança da Informação da Companhia, incluindo mas não se limitando a: perda, furto ou roubo, deverá ser reportado conforme diretrizes da NOR-032 Norma de Resposta a Incidentes de Segurança da Informação.

q) A adoção de medidas de ajuste relacionadas à Segurança da Informação que se fizerem necessárias em decorrência dos incidentes ocorridos será de responsabilidade do Gestor da Área de TI, cabendo ao próprio operacionalizá-las.

r) Quaisquer mudanças nos processos e rotinas da Companhia devem ser realizadas em conformidade com esta política.

s) Os Funcionários e Terceiros devem zelar para que Material de Conteúdo Inadequado não seja exposto, armazenado, distribuído, editado ou gravado.

t) Visando a proteção das Informações da Companhia de Ataques Cibernéticos, a Área de TI deverá manter ativas ferramentas de controle de tráfego da internet, filtragem de e-mails, proteção de dispositivos e Informações, e de isolamento/restrição de acesso a suas redes internas.

u) É terminantemente proibido divulgar ou compartilhar comentários, mensagens ou discussões sobre a Companhia, seus clientes, e seus investidores, assim como Informações da Companhia, conforme sua classificação, através de redes sociais, salas de bate-papo, websites e blogs, a menos que expressamente autorizado pela Área de Comunicação.

v) Os arquivos contidos na pasta pública são para utilização temporária e serão excluídos pela Área de TI periodicamente.

w) Ao utilizar os meios de comunicação e ferramentas de trabalho disponibilizados pela Companhia, as Informações enviadas ou recebidas poderão ser monitoradas e armazenadas a fim de garantir que esses recursos sejam utilizados de forma adequada.

x) No mínimo a cada ano, a Área de TI realizará testes de segurança para os sistemas de Informação.

6.2 Acesso físico

a) Todos os Funcionários e Terceiros deverão portar um crachá de identificação para acesso às dependências da Companhia.

b) Os Terceiros que adentrarem nas dependências da Companhia devem ser previamente cadastrados, identificados e acompanhados pelo Funcionário responsável.

c) As dependências da Companhia devem possuir barreiras físicas, tecnológicas e de monitoramento com objetivo proteger e impedir acessos não autorizados

d) As seguintes áreas devem ter seu acesso restrito e/ou controlado:

- Recursos Humanos;
- Sala de Servidores;
- Centros de Controle Operacional (CCO); e
- Auditoria Interna.

e) Caso não exista separação física para estes ambientes, torna-se ainda mais imprescindível tomar os devidos cuidados com o manuseio, transmissão oral e escrita de Informações, conforme sua classificação..

f) Cabe ao Gestor de cada área tomar todos os cuidados para que aqueles que transitem pelo recinto sejam devidamente informados de que se trata de área com acesso restrito.

g) Somente Funcionários da equipe de Infraestrutura de TI ou pessoas autorizadas pela mesma podem ter acesso à Sala de Servidores da Companhia, as quais devem possuir monitoramento e controle de acesso eletrônico.

h) Somente Funcionários devidamente autorizados pela Área de Operação podem ter acesso à sala do Centro de Controle Operacional, que deve possuir monitoramento e controle de acesso eletrônico.

6.3 Recursos de Tecnologia da Informação

a) As diretrizes, responsabilidades e procedimentos a serem observados em relação ao acesso e utilização dos Recursos de Tecnologia da Informação são definidas e estão disponíveis na NOR 015 – Norma de Segurança e Tecnologia da Informação.

b) As permissões de acesso aos Recursos de Tecnologia da Informação da Companhia devem ser baseadas nas necessidades de negócio, considerando-se o perfil funcional dos Usuários.

c) É responsabilidade de cada Gestor a solicitação formal de liberação, alteração, suspensão ou revogação de acesso dos membros de sua equipe a qualquer Recursos de Tecnologia da Informação.

d) A fim de haver um controle quanto aos direitos de acessos dos Usuários, qualquer mudança de área de atuação ou desligamento deverá ser informado formalmente pelos Gestores das áreas envolvidas à Área de TI, para que sejam tomadas as medidas cabíveis quanto àrevogação ou mudança e permissão do acesso.

e) Toda solicitação de acesso aos Recursos de Tecnologia da Informação deverá ser documentada formalmente e justificada quanto a sua real necessidade, seguindo as diretrizes da NOR-015 Norma de Segurança da Informação.

f) Cada Gestor é reponsável pela solicitação da liberação, alteração, suspensão ou revogação de acesso a qualquer Recurso de Tecnologia da Informação para seus Terceiros contratados, em caso de:

- contratação;
- alteração do escopo dos serviços;
- encerramento das atividades.

g) Os acessos concedidos a Terceiros deverão ter caráter provisório sendo obrigatório ao Gestor responsável pelo mesmo indicar, no ato da solicitação, o prazo limite para utilização dos recursos e a data de encerramento do contrato com o Terceiro.

h) Toda solução de Tecnologia da Informação deve ser homologada pela Área de TI.

i) Apenas os Funcionários da equipe de Infraestrutura de TI, com credenciais privilegiadas, ou pessoas autorizadas pela equipe de Segurança da Informação podem realizar a instalação de softwares homologados pela Companhia e/ou autorizados pela equipe de Segurança da Informação.

j) Apenas os Funcionários da equipe de Infraestrutura de TI, devidamente autorizados, devem executar alterações em softwares e equipamentos corporativos.

k) O Usuário é o responsável pela conservação e integridade dos Recursos de Tecnologia da Informação que utiliza.

l) O Usuário para o qual for disponibilizado notebook e/ou smartphone corporativo deverá assinar o Termo de Responsabilidade específico para estes equipamentos.

m) Nenhum Usuário pode utilizar os recursos da Companhia para deliberadamente propagar qualquer tipo de malware, phishing, spam ou qualquer tipo de programa com um objetivo malicioso.

n) Nenhum Usuário pode utilizar os recursos da Companhia para fazer o download, armazenamento ou distribuição de software pirata. Da mesma forma, não é permitido efetuar Upload de qualquer software licenciado à Companhia ou de dados de propriedade desta ou de seus clientes, sem expressa autorização do Gestor responsável pelo software ou pelos dados.

6.4 Gerência de Usuário e Senha

a) A identificação de acesso aos Recursos de Tecnologia da Informação deve ser efetuada através de uma senha, pessoal e intransferível, criada pelo próprio Usuário, mediante a observância de regras constantes na NOR 015 – Norma de Segurança e Tecnologia da Informação que visam garantir a segurança do acesso e da utilização dos recursos, sendo proibido o seu compartilhamento.

b) O Usuário é responsável por zelar pela confidencialidade e sigilo de suas credenciais (usuários e senhas).

c) Ações realizadas com identificação e senhas do Usuário, como manuseio de dados em arquivos, planilhas eletrônicas e/ou sistemas, serão de inteira e exclusiva responsabilidade do Usuário.

d) Para evitar o acesso indevido de outras pessoas aos Recursos de Tecnologia da Informação, o Usuário deve desligar o computador ou efetuar o bloqueio (CTRL + ALT + DEL e ENTER) sempre que se afastar do equipamento.

e) A Área de TI deve prover mecanismos de segurança que impeça a não utilização de senha em seus Dispositivos Móveis.

f) O compartilhamento de credenciais (usuário e senha) com outras pessoas é terminantemente proibido e está sujeito as penalidades aplicáveis, assim como, o uso de credenciais de outras pessoas.

g) Mecanismos automáticos implantados pela Área de TI bloqueiam as contas de Usuários após tentativas de acesso com senha incorreta. Para solicitar o desbloqueio, é necessário abrir um chamado na Plataforma de Chamados da BRK.

h) A Área de TI também deverá implementar mecanismos automáticos que assegurem a alteração periódica de senha dos Usuários, assim como, permitir que os Usuários possam alterar a própria senha a qualquer momento.

6.5 Internet

a) A internet disponibilizada pela Companhia deverá ser utilizada somente para fins profissionais. Essa regra se estende às redes wi-fi da Companhia.

b) É proibido acessar através dos Recursos de Tecnologia da Informação e demais ferramentas disponibilizadas pela Companhia as seguintes categorias de sites: de apostas, conteúdo adulto, com material obsceno/ofensivo, atividades criminais/ilícitas, armas, violência, expressões de ódio, encontros, jogos, bate-papo (chat), sites que façam ou permitam controle remoto de computadores, hacking, sites com transmissão de som e vídeo ou qualquer outra categoria que não seja para fins profissionais, e outras que vierem a ser bloqueadas.

c) As regras mencionadas nesta política para uso dos Dispositivos Móveis devem ser respeitadas também quando utilizados fora da Companhia.

6.6 E-mail e sistemas de mensagens eletrônicas

a) O E-mail Corporativo deverá ser utilizado exclusivamente para assuntos de negócios relativos à Companhia. Sendo assim, não são permitidos envio de correntes, e-mails de despedida, com palavras de uso inapropriado e/ou com brincadeiras, entre outras sem fins corporativos.

b) Todos os assuntos de negócios devem ser conduzidos pelo E-mail Corporativo da Companhia e/ou por sistemas de mensagens homologados pela Área de TI; portanto, não deve ser utilizado qualquer sistema de mensagem pessoal.

c) A Área de TI deverá ter controles tecnológicos para limitar o tamanho das caixas postais, volume total de mensagens enviadas, quantidade de mensagens armazenadas nos servidores de e-mail, número de destinatários, conteúdo, tamanho e tipo de anexo enviado com a finalidade de garantir o bom funcionamento do serviço de acordo com os recursos disponibilizados, segurança, confidencialidade e privacidade.

d) A qualquer momento que julgar necessário, a Área de TI pode utilizar mecanismos para bloqueio, na entrada ou saída de mensagens, por tamanho, conteúdo, anexos e download de arquivos que não sejam condizentes com as atividades da Companhia.

6.7 Gerência de antivírus

a) Com o objetivo de proteger os Recursos de Tecnologia de Informação da Companhia contra ameaças de malware, phishing, spam ou qualquer tipo de programa com um objetivo malicioso, a equipe de Infraestrutura de TI deve manter atualizada a ferramenta de controle de prevenção e detecção, respeitando no mínimo a periodicidade recomendada pelo fabricante.

6.8 Sistemas de Informação

a) Cabe à Área de TI homologar soluções técnicas e aos Usuários homologar as funcionalidades dos sistemas.

b) As solicitações para desenvolvimento ou contratação de novos sistemas devem ser encaminhadas à Área de TI, que deverá observar as melhores práticas de segurança da Informação.

c) Os Ambientes de Desenvolvimento, Homologação e Produção deverão ser segregados, garantindo assim a integridade dos dados.

d) A Companhia deve, através de seus Gestores, estabelecer prazos e procedimentos para arquivamento e descarte de Informações, Dados Pessoais ou Dados Pessoais Sensíveis, cumprindo com os requisitos legais e regulamentares aos quais é submetida.

e) Todos os programas instalados são registrados, homologados e licenciados, não sendo permitido ao Usuário final:

- instalar qualquer tipo de software não autorizado;
- desativar ou mudar a configuração e/ou parametrização dos programas instalados nos equipamentos disponibilizados;
- desabilitar ou mudar a configuração de qualquer ferramenta ou política de segurança aplicada aos Recursos de Tecnologia da Informação sem a prévia autorização da equipe de Segurança da Informação.

f) A reprodução não autorizada dos softwares instalados nos equipamentos disponibilizados constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

g) É vedada a reprodução e/ou compartilhamento parcial ou total para fora da Companhia de códigos dos sistemas e aplicações desenvolvidas por Funcionários ou Terceiros da Companhia sem um consentimento por escrito da equipe de Segurança da Informação.

6.9 Contingência e continuidade dos principais sistemas e serviços

a) A estrutura de tecnologia da Informação deve possuir mecanismos de contingência, visando reduzir riscos de perda de confidencialidade, integridade, disponibilidade e privacidade dos dados e ou informações. Estes mecanismos devem ser detalhados através de documentos normativos, incluindo um plano de contingência.

6.10 Treinamento e Conscientização

a) A Companhia deve realizar treinamentos de forma regular e periódica, conforme estabelecido pela equipe de Segurança da Informação, a fim de conscientizar todos os seus Funcionários e Terceiros acerca dos temas que envolvem Segurança da Informação. As ações de conscientização devem ser realizadas em diferentes formatos e abranger diferentes públicos, envolvendo treinamentos de modo presencial, online e/ou campanhas informativas.

7. Controle de Registros

Registros não são requeridos por este Instrumento Normativo.

8. Disposições Finais

Esta política entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

9. Controle e histórico de versões

Data	Versão	Sumário
01/11/2017	01-2017	Criação do instrumento normativo
26/11/2019	01-2019	Revisão anual do instrumento normativo
07/12/2020	01-2020	Revisão anual do instrumento normativo
11/11/2022	01-2022	Revisão geral do instrumento normativo
31/01/2024	01-2024	Ajustes no item “Glossário” e inclusão do item “7. Controle de Registros”
30/01/2026	01-2026	Republicação em igual teor

10. Aprovações

Código	Descrição	Versão	Vigência
POL-002	Política de Segurança da Informação	01-2026	30/01/2026 a 30/01/2028

Aprovador(es): Conselho de Administração