Política de Segurança de Bens de Informação

Potássio do Brasil Ltda.

Outubro de 2022

SUMÁRIO

1. INTRODUÇÃO

Toda e qualquer informação utilizada pela **Potássio do Brasil Ltda.** ("**PdB**") tem valor e deve ser protegida, cuidada e gerenciada de forma a garantir sua disponibilidade, integridade, confidencialidade, legalidade, rastreabilidade e a possibilidade de ser auditada, independentemente do meio onde estiver armazenada.

Nesse contexto, a **Potássio do Brasil** elaborou sua Política de Segurança de Bens de Informação ("Política"), seguindo as melhores práticas internacionais para garantir a adequada segurança de suas informações.

Esta Política está diretamente relacionada com o Código de Conduta da **Potássio do Brasil**. Todos os colaboradores, incluindo consultores e contratados ("colaboradores"), deverão cumprir o disposto nesta Política, por meio da utilização adequada de recursos tecnológicos, equipamentos e softwares. Se for identificada pelo colaborador a possibilidade de promover melhorias nesta Política, é dever de cada um fazer a imediata comunicação ao Comitê de Compliance, através do e-mail compliance@potassiodobrasil.com.br.

Os colaboradores da **Potássio do Brasil** serão cientificados sobre esta Política, receberão treinamento e serão informados sobre os locais onde ela pode ser acessada e/ou impressa. A última página deverá ser preenchida de próprio punho, assinada e entregue a qualquer membro do Comitê de Compliance. Este protocolo será arquivado na ficha de cada colaborador ou no contrato de prestação de serviços, conforme o caso.

O não cumprimento das orientações desta Política, por qualquer colaborador, independentemente do motivo, será base para adoção das medidas disciplinares cabíveis pelo Comitê de Compliance. Eventual exceção que direcione ao não cumprimento de qualquer orientação prevista nesta Política, somente poderá ser feita se prévia e formalmente aprovada pelo Comitê de Compliance.

2. OBJETIVO

Esta Política visa regular a relação da **Potássio do Brasil** com seus colaboradores – definidos no tópico 3 – em relação aos bens de informação pertencentes ou que são disponibilizados pela **Potássio do Brasil** para a operação dos negócios da **Potássio do Brasil**.

Como **Bens de Informação** devem ser entendidos todos os recursos disponibilizados (micros, software, rede de comunicação, telefonia, correio eletrônico e outros) e todos os dados e informações independentemente da forma como são armazenados (papel, HD´s pessoais ou corporativos, bases de dados corporativas *[File Server, Sharepoint, FTP, SQL DataBase]*, pen drive, CDs e outros).

Nos tópicos abaixo serão descritas as principais orientações e definições sobre como a **Potássio do Brasil** deseja que seus colaboradores ajam em relação aos **Bens de Informação** que são disponibilizados pela **Potássio do Brasil** para a adequada execução dos trabalhos delegados e previstos para cada um, independentemente de seu cargo ou posição hierárquica.

3. PÚBLICO-ALVO

Esta Política se aplica a todos os colaboradores da **Potássio do Brasil** (celetistas ou terceiros), custodiantes das informações (equipe de Tecnologia da Informação para os ambientes corporativos e usuários para os equipamentos de uso individual), gestores dos dados e informações (geradores de dados e informações que serão arquivadas nos equipamentos da **Potássio do Brasil** ou de qualquer empresa do Grupo Forbes & Manhattan) e Diretoria Executiva (todos em conjunto “Colaboradores”).

Para fins desta Política, entende-se como empresas do Grupo Forbes & Manhattan todas aquelas que estão sob gestão, direta ou indireta, do escritório administrativo de Belo Horizonte e/ou de Toronto (Canadá), incluindo, mas sem se limitar a: Forbes & Manhattan, Brazil Potash. e Potássio do Brasil Ltda. As empresas, escritórios ou novas unidades porventura criadas que compartilhem quaisquer **bens de Informação** da **Potássio do Brasil** devem aderir, imediata e automaticamente, ao Programa de Compliance da **Potássio do Brasil**.

4. USO DO E-MAIL CORPORATIVO DA POTÁSSIO DO BRASIL

O e-mail corporativo da **Potássio do Brasil** é a forma de comunicação entre computadores, usando software próprio. As mensagens poderão ser redigidas e lidas em equipamentos pessoais dos Colaboradores, porém não mantidas e arquivadas exclusivamente nestes equipamentos. O uso do e-mail corporativo deve ser feito exclusivamente para atender aos interesses da **Potássio do Brasil**.

a) O que posso e devo fazer

i. Enviar mensagens para usuários internos ou externos relativas aos negócios da **Potássio do Brasil** e no interesse da empresa.
ii. Escrever as mensagens em linguagem clara, objetiva, sem vícios, jamais ofensivas e respeitando os princípios da boa conduta e ética.
iii. Remover as mensagens que não são uteis ou que perderam a validade aos negócios da **Potássio do Brasil**, em especial as caixas de lixo eletrônico e excluídos.
iv. Enviar cópia de mensagens somente às pessoas que realmente precisam conhecer ou tomar uma decisão sobre o assunto tratado;
v. Sempre utilizar a assinatura eletrônica padrão determinada pela **Potássio do Brasil** nas mensagens enviadas, com as variáveis de empregado e prestador de serviços;
vi. Manter o texto do “aviso legal” ou “*disclaimer*” determinado pela **Potássio do Brasil** nas mensagens enviadas, se assim for exigido.

b) O que não posso fazer

i. Expor a imagem ou opinião da **Potássio do Brasil** sobre qualquer assunto, exceto se previamente autorizado pelo superior hierárquico.
ii. Usar o e-mail corporativo para assuntos particulares e usar o e-mail pessoal para assuntos atinentes à **Potássio do Brasil**. Exceções poderão ser toleradas, desde que não comprometam a operação e a segurança dos sistemas da empresa, o que poderá ser identificado pelo monitoramento das mensagens transitadas nos equipamentos da empresa.
iii. Escrever ou reencaminhar mensagens recebidas, por meio do e-mail corporativo, que não estejam diretamente ligadas aos negócios da **Potássio do Brasil**, em especial as que menosprezem, depreciem pessoas físicas ou quaisquer instituições, ou que estejam

relacionadas a racismo, orientação sexual, idade, religião, nacionalidade, deficiência física, partido político.

iv. Enviar mensagens com conteúdo ilícito ou ofensivas, para comercialização de produtos, ou relacionadas a atividades proibidas por lei, por esta Política e pelo Código de Conduta da **Potássio do Brasil**.

v. Aceitar ou abrir arquivos, fotos, hiperlinks, software – mesmo os demos – de usuários desconhecidos.

vi. Encerrado o vínculo com a **Potássio do Brasil**, fazer ou manter consigo back-up do e-mail corporativo, salvo autorização prévia e por escrito da Diretoria.

5. ACESSO À INTERNET

Acesso à rede internacional de computadores (www – world wide web, também conhecida como sites de Internet) é uma ferramenta poderosa para agilizar a comunicação e informação entre pessoas físicas. O uso da Internet deve ser feito exclusivamente para atender aos interesses da **Potássio do Brasil**, independentemente do meio usado para o uso desta ferramenta (microcomputadores, tablets, celulares).

O acesso a alguns sites de interesse pessoal podem ser tolerados, desde que não comprometa o bom andamento das atividades da **Potássio do Brasil**, por exemplo, desenvolvimento pessoal e profissional em assuntos relacionados aos objetivos da empresa.

a) O que posso fazer

i. Acessar sites que de alguma forma facilite o andamento dos negócios da **Potássio do Brasil**;

ii. Usar somente o software de navegação homologado e autorizado, que é controlado pela área de Tecnologia da Informação da empresa.

b) O que não posso fazer

i. Navegar em sites de conteúdos não confiáveis, ou mesmo em sites de conteúdos que não agreguem valor ao exercício de suas funções na empresa.

ii. Repassar informações consideradas confidenciais e que de alguma forma possam prejudicar os negócios da **Potássio do Brasil**.

iii. Desabilitar ou alterar qualquer configuração ou produto de proteção de navegação na Internet, tais como softwares antivírus, de controle de acesso a sites proibidos, de controle de saída de dados e informações.

iv. Executar qualquer ação que possa de alguma forma infringir direitos autorais, marcas, licenças, patentes ou que possam ser entendidas como ofensivas a qualquer pessoa, em especial assuntos relacionados a credo, sexo, religião, partidos políticos, racismo ou outros.

v. Divulgar propaganda pessoal ou comercial da **Potássio do Brasil** ou de outras empresas do grupo, sem prévia e expressa autorização da Diretoria.

vi. Instalar programas e baixar softwares em computadores da **Potássio do Brasil** sem prévia autorização da TI.

6. CLASSIFICAÇÃO E ACESSO À INFORMAÇÃO

As informações da **Potássio do Brasil** podem ser classificadas de acordo com sua criticidade aos negócios. Esta classificação é definida pelo responsável no momento de sua criação e

inclusão nos arquivos corporativos. São três classificações possíveis:

(a) Restrita à Diretoria;
(b) Confidencial e de segurança da operação da **Potássio do Brasil**; e
(c) Públicas.

Não havendo classificação, a informação deve ser considerada pelos interlocutores como confidencial e de segurança para a operação da **Potássio do Brasil**.

O acesso às informações pode ser monitorado pela Equipe de Tecnologia da Informação, pela Diretoria e pelo Comitê de Compliance sempre que for necessário.

a) O que posso fazer

i. Acessar somente os dados e informações aprovadas e disponibilizadas para o meu perfil de acesso, com minha identificação (meu ID e senha).
ii. Informar de imediato ao seu superior hierárquico o eventual acesso a dados e informações que julgar não autorizado.
iii. Manter as cópias de segurança, conforme definições e orientações da área de Tecnologia da Informação.
iv. Acatar as inclusões, exclusões e alterações de acesso às informações do Grupo, conforme definição do seu superior hierárquico.

b) O que não posso fazer

i. Acessar dados e informações que estejam em desacordo com meu perfil de acesso.
ii. Arquivar informações pessoais exclusivamente nos equipamentos da **Potássio do Brasil**, uma vez que empresa tem livre acesso aos dados existentes em equipamentos de sua propriedade, podendo apagá- los ou monitorá-los, a qualquer tempo, sem prévia consulta ao colaborador.[1]
iii. Manter informações pessoais de caráter sigiloso em bases de dados de qualquer equipamento da **Potássio do Brasil**, já que tais bases de dados são constantemente monitoradas pela equipe de TI ou da empresa.
iv. Manter informações da **Potássio do Brasil** em equipamentos pessoais, exceto para as pessoas que forem formalmente autorizadas pelo Superior Hierárquico ou pelo Comitê de Compliance, dependendo do caso.
v. Encaminhar mensagens classificadas como “Restrita a Diretoria” ou “Confidencial e de segurança da operação da **Potássio do Brasil**” para colaboradores ou terceiros que não possuem autorização de acesso a esta informação;
vi. Recusar ou de qualquer forma impedir o monitoramento de acesso às informações residentes em bases de dados de qualquer equipamento da **Potássio do Brasil**, pela equipe de TI ou terceiros autorizados pela **Potássio do Brasil**.

7. USO DOS RECURSOS DE INFORMÁTICA

A **Potássio do Brasil** fornece todos os recursos de informática (“recursos”) necessários para que seus Colaboradores possam executar suas atividades

[1] O empregado que manter informações pessoais exclusivamente no computador do Grupo, deverá fazê-lo em uma pasta separada, nominal, consciente de que, em caso de pane ou necessidade de espaço nos servidores, poderá ter sua pasta excluída sem aviso e sem a possibilidade de realização de back-up profissionais. Estes recursos devem ser utilizados somente para as atividades relacionadas aos negócios da **Potássio do Brasil**, de acordo com as regras e procedimentos previstos no Termo de Custódia de Equipamentos assinado pelo detentor do equipamento e na presente Política.

a) O que devo fazer

i. Garantir a integridade e funcionalidade dos recursos disponibilizados, tanto os hardwares quanto softwares e demais equipamentos que estão sob sua custódia, tanto no ambiente da **Potássio do Brasil** quanto em trânsito.
ii. Devolver de imediato os recursos à **Potássio do Brasil** em eventual rompimento da relação profissional.
iii. Disponibilizar, permanentemente, os recursos para monitoramento de seu conteúdo ao pessoal de TI ou para terceiros formalmente autorizados pelo Comitê de Compliance.
iv. Seguir as regras de proteção das informações definidas pelo Comitê de Compliance e pela equipe de TI, tais como criptografia dos dados e informações restritas e sensíveis.
v. Informar a equipe de TI se notar qualquer situação anormal no funcionamento dos recursos.
vi. Informar a equipe de TI, no primeiro momento possível, a suspeita de roubo ou perda de um recurso da **Potássio do Brasil**.
vii. Usar os recursos de impressão e xerox com moderação e somente em casos de reconhecida necessidade da **Potássio do Brasil**.
viii. Buscar substituição de impressão e xerox, sempre que possível, por uso de meio magnético (por exemplo, evitar a impressão ou xerox com objetivo de leitura e correção do documento).

b) O que não posso fazer

i. Aproximar os recursos de imãs ou expô-lo a calor ou frio excessivo ou de rede elétrica de alta voltagem.
ii. Alterar qualquer configuração dos recursos, exceto se autorizado e sob o rigoroso acompanhamento da equipe de TI.
iii. Ceder ou facilitar o acesso de terceiros aos recursos que estão sob sua custódia.
iv. Imprimir documentos pessoais em cores.
v. Usar meios de impressão, xerox e telefonia da **Potássio do Brasil** para qualquer atividade não relacionada aos interesses da **Potássio do Brasil**, observado sempre o bom senso. Serão considerados abusos, por exemplo, a impressão de monografias e teses não relacionados aos negócios, impressão de fotos pessoais e outros.

8. COPIAS DE SEGURANÇA DOS DADOS E INFORMAÇÕES DO GRUPO

Os equipamentos que mantêm dados e informações são suscetíveis a quebras e travamento físico de acesso às bases de dados e sistemas. Todos os dados e informações classificados como restritos ou confidenciais, importantes para a operação da **Potássio do Brasil**, devem ter uma cópia de segurança em local distinto do original onde está armazenado.

a) O que devo fazer

i. Seguir as orientações da equipe de TI quanto à:
   a. Obrigatoriedade de salvar os documentos profissionais e pessoais nos locais indicados pela Equipe de TI da **Potássio do Brasil**.
   b. Validade das informações para a **Potássio do Brasil**, transferindo-as para pastas de arquivo de uso secundário (arquivo morto) ou deletando-os.
ii. Manter as cópias de segurança em ambiente físico adequado.
iii. Testar a recuperabilidade das informações de segurança a cada seis meses.
iv. Facilitar o acesso das cópias de segurança para atividades de monitoramento e auditoria.

b) O que não posso fazer

i. Manter cópias em local ou meio de armazenamento não autorizado pela equipe de TI da **Potássio do Brasil**.
ii. Enviar dados e informações para terceiros sem autorização da **Potássio do Brasil**.
iii. Criptografar e proteger dados e informações com senhas contra acesso de terceiros em desacordo com orientações da equipe de TI.

9. USO DE PROGRAMAS E SISTEMAS NOS COMPUTADORES

A **Potássio do Brasil** fornece aos seus Colaboradores todas as ferramentas que necessitam para a correta execução de suas atividades operacionais. O uso dos programas e sistemas deve ser feito exclusivamente para atender aos interesses da **Potássio do Brasil**.

a) O que devo fazer

i. Usar somente os programas e sistemas homologados e autorizados pela área de TI.
ii. Manter e acompanhar a atualização dos sistemas, em especial o antivírus, no caso de microcomputadores.
iii. Solicitar à equipe de TI que remova programas e sistemas que não possuem utilidade – ou perderam sua utilidade operacional para os do Grupo Forbes&Manhattan.

b) O que não posso fazer

i. Instalar, ou permitir a instalação de programas e sistemas não homologados e autorizados pela área de TI da **Potássio do Brasil**
ii. Instalar, permitir a instalação ou aceitar programas e sistemas recebidos pela Internet, independentemente se legalmente autorizados ou “free”.
iii. Instalar, permitir a instalação ou aceitar o uso de programas sem licença legal (software pirata) independentemente do motivo.

10. USO DE SENHAS PARA O ACESSO LÓGICO

O acesso aos computadores e às bases de dados corporativas ou residentes nos computadores cedidos ao usuário pela **Potássio do Brasil** deve ser feito exclusivamente com identificação pessoal do usuário e respectiva senha (ID + senha de acesso).

É responsabilidade de cada Colaborador garantir a confidencialidade de suas senhas de acesso e seguir os procedimentos de segurança estabelecidos pela Equipe de TI da **Potássio do Brasil**. O compartilhamento de senhas coloca em risco a segurança das informações, além de comprometer o detentor da senha, caso haja uso indevido, sendo considerada falta grave de segurança.

a) O que devo fazer

i. Manter sua senha de acesso aos recursos de informática sob seu exclusivo domínio; a senha é pessoal e intransferível.
ii. Usar senhas com mescla de números, letras e símbolos especiais (vírgula, ponto e vírgula, dois pontos, por exemplo) e no tamanho definido pela equipe de TI da **Potássio do Brasil**
iii. Trocar sua senha a cada 03 (três) meses ou a qualquer momento caso perceba o risco de que algumas outras pessoas possam ter o conhecimento de sua senha.

iv. Trocar a primeira senha de acesso cedida pela equipe de TI da **Potássio do Brasil** (senha descartável), antes de iniciar o uso dos recursos de informática.
v. Respeitar as regras de bloqueio automático de tentativas de acesso sem sucesso e solicitar apoio da equipe de TI sempre que necessário.

b) O que não posso fazer
i. Ceder sua senha para terceiros, subordinados, superiores hierárquicos ou equipe de TI, independentemente do motivo.
ii. Registrar ou anotar sua senha em local que outras pessoas possam ter acesso.
iii. Ceder senhas de acesso wi-fi para pessoas não autorizadas.

11. ACESSO REMOTO AOS COMPUTADORES PELA EQUIPE DE TI

O acesso remoto é uma ferramenta que permite à equipe de TI da **Potássio do Brasil** fazer ajustes nos recursos computacionais à distância. Em casos pontuais, o acesso aos computadores dos Colaboradores pode ser solicitado pela equipe de TI, em especial para:

i. Manutenção remota (a partir da sede da **Potássio do Brasil**);
ii. Atualização de programas, sistemas ou bases de dados; ou
iii. Monitoramento dos sistemas, programas, bases de dados ou auditoria.

a) O que devo fazer
i. Liberar o acesso, seguindo as instruções técnicas da equipe de TI da **Potássio do Brasil**.
ii. Ter certeza de que os dados críticos ou confidenciais não estão disponíveis no computador. Proceder o imediato bloqueio do acesso remoto, assim que as atividades da equipe de TI forem concluídas;
iii. Usar apoio da equipe técnica em caso de dúvidas neste procedimento.

b) O que não posso fazer
i. Liberar acesso remoto a pessoas não autorizadas, independentemente do motivo.
ii. Dificultar o acesso remoto para a equipe de TI da **Potássio do Brasil** ou para quem o Comitê de Compliance formalmente autorizar.

12. REGISTRO DE INCIDENTES DIVERSOS

Independentemente dos esforços da **Potássio do Brasil** e da equipe de TI, falhas e problemas nos recursos de TI são esperados e normais. Todo incidente, que de qualquer forma, prejudique o bom andamento dos negócios da **Potássio do Brasil** devem ser reportados, solucionados e acompanhados pelos respectivos usuários e pela equipe de TI.

a) O que devo fazer
i. Reportar para equipe de TI da **Potássio do Brasil** qualquer indício de incidente que possa afetar a operação dos seus negócios.
ii. Acompanhar os ajustes que serão feitos ou orientados pela equipe de TI da **Potássio do Brasil**.
iii. Tratar os ajustes eventualmente necessários decorrentes do incidente.

b) O que não posso fazer
i. Ocultar o reporte de incidentes conhecidos relacionados aos recursos disponibilizados

para as atividades operacionais da **Potássio do Brasil**.

13. DOCUMENTOS EM PAPEL OU ARQUIVADOS EM MÍDIAS MOVEIS

Embora a **Potássio do Brasil** – e o mundo – estejam caminhando para que todos os seus Bens de Informação estejam arquivados em meios magnéticos e com acesso controlado por identificação de usuário e senha pessoal, as informações restritas ou confidenciais podem, de alguma forma e por qualquer motivo, estarem impressas em papel ou outro meio; o que deve ser rigorosamente controlado pelos usuários.

a) O que posso fazer

i. Evitar o registro de informações restritas e confidenciais em papel. Caso seja necessário, sinalizar, por escrito, a confidencialidade e arquivá-lo em local restrito. Destruir adequadamente as informações consideradas inservíveis aos interesses do Grupo Forbes&Manhattan (usando fragmentadora por exemplo).
ii. Descartar o lixo, na medida do possível, de forma a seguir as melhores regras de reciclagem.

b) O que não posso fazer

i. Descartar em lixo ou em caixas de rascunhos papéis ou arquivos sem que estejam adequadamente inutilizados.

14. SEGURANÇA FÍSICA

Todos os recursos cedidos aos Colaboradores (microcomputadores, máquinas de xerox, impressoras, roteadores, computadores de médio porte, centrais de telefonia, centrais elétricas, distribuidores de rede elétrica, telefonia, periféricos e etc.) devem ser preservados de acordo com as melhores práticas de acesso físico.

Somente deve ter acesso aos recursos físicos, o pessoal autorizado ou terceiros com prévio e formal autorização da equipe de TI da **Potássio do Brasil**.

Os locais físicos onde os Bens de Informação são localizados devem ter acesso restrito, protegidos contra invasões e acessos não autorizados, controlados, limpos, secos e adequadamente monitorados.

a) O que posso fazer

i. Acessar somente os recursos disponibilizados pela **Potássio do Brasil** para o exercício das atividades profissionais por ela previstas.
ii. Informar a equipe de TI a eventual liberação – ou poder de acesso – a locais físicos ou recursos não necessários às atividades operacionais da **Potássio do Brasil**.
iii. Manter o local físico necessário para as atividades operacionais, na medida do possível: limpos, desinfetados, sem poeira, sem umidade.
iv. Travar o acesso aos equipamentos quando se ausentar da estação de trabalho.

b) O que não posso fazer

i. Acessar, por qualquer motivo, locais físicos não necessários para o exercício das atividades contratadas com a **Potássio do Brasil**.

15. MONITORAMENTO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Seguindo as melhores práticas usuais da Boa Governança Corporativa e de Tecnologia da Informação, a **Potássio do Brasil** poderá, independentemente de qualquer comunicação prévia ou autorização do Colaborador, monitorar, fiscalizar e acessar todas as atividades e informações trafegadas e arquivadas em recursos de propriedade da **Potássio do Brasil**, durante ou após o encerramento da relação profissional.

a) Monitoramento

i. A **Potássio do Brasil** se reserva o direito ao monitoramento de uso de todos os recursos pertencentes e/ou disponibilizados pelo Grupo aos seus Colaboradores, como micros, software, arquivos residentes nos micros, arquivos residentes em bases corporativas, dentre outros.

ii. Também poderão ser monitorados os processos de comunicação – e-mail corporativo, telefonia e outros, a qualquer tempo, durante ou após o encerramento da relação de trabalho, independentemente de prévia comunicação ou autorização.

iii. As atividades de monitoramento poderão ser executadas pela equipe de TI ou por terceirizados contratados pela **Potássio do Brasil** com propósito específico, de forma preventiva, corretiva ou detectiva, eventual ou permanente (auditorias pontuais ou monitoramento contínuo por ações pessoais ou por softwares específicos para este fim), local ou remotamente.

b) Legalidade do monitoramento

i. A possibilidade deste monitoramento é reconhecida e aceita por todos os Colaboradores da **Potássio do Brasil** – celetista ou terceirizados, o que é evidenciado formalmente a partir da assinatura do Termo de Responsabilidade, descrito na última página desta Política.

16. PROPRIEDADE INTELECTUAL

O Colaborador deve estar ciente de que as ideias, invenções, inovações, tecnologias, conhecimentos, know-how, dados técnicos, informações de processos e de mercado desenvolvidos durante a relação de trabalho, mesmo que individualmente, são de propriedade da **Potássio do Brasil**, sendo assim entendida propriedade industrial ou intelectual.

A propriedade industrial e a intelectual são ativos de valor imprescindível para a **Potássio do Brasil** e possuem caráter confidencial.

O uso ou a divulgação não autorizada de propriedade industrial ou intelectual da **Potássio do Brasil** violam a presente Política e constituem falta grave, podendo resultar em consequências negativas, tanto para a **Potássio do Brasil** quanto para os Colaboradores e Terceiros envolvidos, incluindo ações judiciais e disciplinares.

Da mesma forma, é exigido dos Colaboradores e Terceiros o respeito ao direito de propriedade de outras empresas e suas informações exclusivas.

17. RESPONSABILIDADES E PENALIDADES

O não cumprimento de qualquer parte desta Política de Bens de Informação poderá gerar medidas orientativas e disciplinares, inclusive com demissão por justa causa (no caso de empregado) ou rescisão contratual (no caso de terceiros), a critério da Diretoria Executiva em conjunto com o Comitê de Compliance da **Potássio do Brasil**.

18. DÚVIDAS, SUGESTÕES E REVISÃO DA POLÍTICA DE SEGURANÇA DE BENS DE INFORMAÇÃO

a) Revisão da Política

i. Esta Política será revisada a cada 12 meses, atividade que será coordenada pelo Comitê de Compliance e executada pela equipe de TI.

ii. A critério exclusivo do Comitê de Compliance, esta revisão poderá ser executada a qualquer tempo, dependendo da relevância das modificações para a segurança das informações do Grupo.

b) DÚVIDAS E SUGESTÕES

As dúvidas que surgirem na aplicação das diretrizes desta Política ou em relação a situações não previstas podem ser esclarecidas com o Gestor de cada área, com o Departamento Jurídico ou com o Comitê de Compliance da **Potássio do Brasil**, através do e-mail compliance@potassiodobrasil.com.br.

A **Potássio do Brasil** também aprecia e valoriza o envio de sugestões para atualização e melhoria desta Política, como a inclusão de assuntos não previstos no documento, revisão de conteúdo, entre outras. Tais sugestões devem ser encaminhadas ao Comitê de Compliance, através dos e-mails do e-mail compliance@potassiodobrasil.com.br, bem como depositadas nas caixas de sugestões disponíveis no escritório.

Documento criado em 21 de Outubro de 2022 e aprovado por:

POTÁSSIO DO BRASIL
potassiodobrasil.com.br

Adriano Espeschit
Presidente / President

ANEXO I
TERMO DE RESPONSABILIDADE DO USUÁRIO

(Via destacável para assinatura e entrega ao RH)

Declaro que li, entendi, concordei e não tenho dúvidas quanto ao conteúdo da Política de Segurança de Bens de Informação da Potássio do Brasil.

Declaro ainda que tenho ciência de que:

I. Dados e informações pessoais não devem ser armazenadas, exclusivamente, nas bases de dados do Grupo, uma vez que esta poderá acessá-los ou apagá-los a qualquer tempo, independentemente de prévia consulta ou autorização. Se forem armazenados, automaticamente estou autorizando que sejam acessados pelo Departamento de TI, Comitê de Compliance ou Diretoria.
II. Não devo usar recursos a mim disponibilizados pela Potássio do Brasil para atividades pessoais ou qualquer outra que não esteja em harmonia com as atividades profissionais para que fui contratado, observado sempre o bom senso.
III. Não devo ter expectativa de privacidade em relação aos recursos a mim confiados pela Potássio do Brasil, especialmente sobre o uso de e-mail corporativo e acessos via internet.
IV. Devo informar imediatamente ao Departamento de TI ou ao remetente, conforme o caso, eventual acesso à informação que não estejam diretamente relacionadas às minhas responsabilidades profissionais.
V. O não cumprimento desta Política, intencionalmente ou não, poderá gerar penalidades conforme entendimento da Potássio do Brasil, ouvido o Comitê de Compliance, inclusive com rescisão contratual (no caso de terceiros) ou demissão por justa causa (no caso de funcionários).

Local , ____ de _____de 20___.

_____
Nome do Colaborador:
CPF:
RG:
Identificação funcional ou contrato de prestação de serviço: