POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
INSTITUTO COMBUSTÍVEL LEGAL

CAPÍTULO I – DOS OBJETIVOS E ALCANCE

A informação é um ativo importante e essencial para o **Instituto Combustível Legal (ICL)**, devendo ser adequadamente protegida para garantir o uso somente por pessoas autorizadas.

A Política de Segurança da Informação estabelece normas, métodos e procedimentos que devem ser seguidas para preservar as informações, protegendo a documentação, os equipamentos, os softwares e as instalações e detectando, impedindo e documentando possíveis ameaças aos ativos do **ICL**.

Para assegurar os processos de proteção das informações, a Política de Segurança da Informação está fundamentada nos seguintes pilares:

- **Disponibilidade:** as informações deverão estar disponíveis para as pessoas autorizadas sempre que necessárias para uso.
- **Integridade:** as informações não deverão ser acessadas, alteradas indevidamente ou violadas e deverão ter conteúdo idôneo. Toda e qualquer informação manipulada deve manter todas as características originais, o que inclui controle de mudanças e garantia do seu ciclo de vida (criação, manutenção e destruição) para que não seja alterada.
- **Confidencialidade:** as informações somente deverão ser acessadas e transmitidas por pessoas autorizadas a terceiros igualmente autorizados a recebê-las, para que não sejam conhecidas, de forma acidental ou proposital, por quem não detém autorização para tanto. A confidencialidade deverá ser garantida por meio de controle de acesso, utilização de metodologias para garantia do ciclo de vida da informação e proibição de divulgação não permitida.
- **Autenticidade e Auditabilidade**: todo acesso e uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi realizado com a informação.
- **Legalidade:** o conteúdo das informações deve estar em consonância com as leis, regulamentos e normas, inclusive de Defesa da Concorrência e Anticorrupção, bem como ao Código de Integridade e Conduta do **ICL** e a presente Política de Segurança da Informação.

A Política de Segurança da Informação se aplica aos COLABORADORES e terceiros e deve ser observada dentro e fora das instalações do **ICL**, em todos os procedimentos, incluindo, mas não se limitando às trocas de informações faladas ou escritas, ao envio e recebimento de mensagens, ao envio e recebimento de e-mails, às conversas telefônicas, à guarda e ao arquivamento de documentos eletrônicos e físicos e à utilização de softwares e hardwares.

O conteúdo da Política de Segurança da Informação é amplamente divulgado aos COLABORADORES e terceiros e totalmente disponibilizado para consulta.

CAPÍTULO II - DEFINIÇÕES

Para melhor compreensão da presente Política, ficam estabelecidas as seguintes definições:

- **Aplicativos de Mensagens:** *whatsapp, telegram, facetime, skype, facebook, messenger, instagram, twitter* e outros que tenham finalidade igual ou similar.
- **Associados:** COLABORADORES das empresas associadas ao **ICL**.

- **Ativos de Tecnologia de Informação:** equipamentos fixos (computador, impressoras, etc.), equipamentos móveis (smartphone, notebooks, tablets, etc.), demais equipamentos de propriedade do **ICL**, e-mails e os softwares utilizados pelo **ICL**. Denominados nesta Política somente como Ativos de TI.
- **Colaboradores:** membros da Assembleia Geral, do Conselho Deliberativo, do Conselho Superior, do Conselho Fiscal, o Diretor, membros do Comitê de Integridade e Conduta e dos Comitês e Grupos de Trabalho, quando houver, os empregados, os estagiários (Lei nº 11.788/2008) e os jovens aprendizes (Lei n º 11.097/2000).
- **Sistema ICL:** Site onde estão armazenados e organizados os arquivos de dados e informações do ICL, que utiliza a plataforma SharePoint Online.
- **TI - Tecnologia de Informação:** conjunto de todas as atividades e soluções providas por recursos de computação que visam à produção, ao armazenamento, à transmissão, ao acesso, à segurança e ao uso das informações.
- **Terceiros:** pessoas físicas ou jurídicas fornecedoras e que prestam serviços ao **ICL**, incluindo, mas não se limitando aos advogados, consultores, assessores, contadores, parceiros etc.

CAPÍTULO III – RESPONSABILIDADES

É dever de todos os COLABORADORES e TERCEIROS, além de cumprir a legislação vigente, o Código de Integridade e Conduta e as demais responsabilidades dispostas na presente Política:

- Garantir o cumprimento da Política de Segurança da Informação do **ICL** e assinar o Termo de Recebimento e Compromisso (anexo 1). A não observância do disposto na Política será de única e exclusiva responsabilidade do COLABORADOR e TERCEIRO.
- Proteger as informações relacionadas ao **ICL**, sendo vedados o acesso, a alteração, a destruição ou a divulgação não autorizada pelo **ICL**.
- Utilizar, de forma falada ou escrita, as informações produzidas, mantidas, recebidas, transmitidas ou obtidas relacionadas ao **ICL** unicamente para atender aos interesses institucionais do **ICL**.
- Não utilizar, informações produzidas, mantidas, transmitidas ou obtidas relacionadas ao **ICL** em ambientes públicos (elevadores, aviões, restaurantes, encontros sociais, táxi etc.).
- Contatar imediatamente o gestor imediato sempre que tomarem conhecimento de incidentes, vulnerabilidades, indícios de comprometimento das informações e Ativos de TI, bem como violação da Política de Segurança da Informação.
- Garantir que o conteúdo das informações que está armazenando, transmitindo, recebendo, produzindo ou alterando, relacionadas ao **ICL** ou em seus Ativos de TI, esteja de acordo com a Política de Segurança da Informação. Eventuais inadequações serão de única e exclusiva responsabilidade do COLABORADOR e/ou TERCEIRO.
- Buscar orientação do Conselho Fiscal e, quando houver, do Comitê de Integridade e Conduta em caso de dúvidas relacionadas à Política de Segurança da Informação.Nos casos permitidos, as informações produzidas, mantidas ou obtidas por meio do **ICL** devem ser utilizadas para atender as finalidades do Instituto e não devem ser compartilhadas, sob nenhuma hipótese, com terceiros sem a prévia autorização.

É dever de todos os COLABORADORES, além de cumprir a legislação vigente, o Código de Integridade e Conduta e as demais responsabilidades dispostas na presente Política:

- Assegurar que os Ativos de TI à sua disposição, sejam unicamente utilizados para fins profissionais e para a execução das atividades institucionais do **ICL**. É expressamente proibido o uso dos Ativos de TI para uso pessoal.

CAPÍTULO IV – DISPOSIÇÕES GERAIS

- A Política de Segurança da Informação pode ser revista a qualquer momento, mas nunca em intervalo superior a dois anos.
- Casos excepcionais ou não contemplados pela Política de Segurança da Informação devem ser tratados individualmente, mediante orientação do Conselho Fiscal e, quando houver, do Comitê de Integridade e Conduta.
- O **ICL** pode, a seu critério, monitorar e registrar a manipulação de dados armazenados ou em trânsito, com o objetivo de zelar pelo fiel cumprimento da Política Corporativa de Segurança da Informação.

CAPÍTULO V – CONTROLE DE ACESSO À INFORMAÇÃO

SEÇÃO I – CREDENCIAIS DE ACESSO

- Todos os COLABORADORES deverão possuir cadastro de credenciais (nome completo, CPF, RG, empresa, telefone e e-mail) de acesso, que será vinculado a uma senha de uso pessoal e intransferível.
- É proibida a utilização não autorizada de credenciais e privilégios de acesso, bem como de quaisquer recursos, físicos ou lógicos, para suprimir controles de acesso vigentes.
- A concessão e a revogação de acesso devem ser registradas de modo que seja possível determinar a data da ocorrência, os COLABORADORES afetados, assim como os privilégios concedidos e revogados.
- O acesso de COLABORADORES desligados do **ICL** deve ser revogado no momento da comunicação do desligamento.
- As credenciais de acesso dos COLABORADORES que encerraram suas atividades no **ICL** não devem ser removidas das bases cadastrais, mas devem ser bloqueadas de forma que não seja possível utilizá-las.
- Devem ser mantidos registros que permitam identificar os COLABORADORES responsáveis pelas ações realizadas por meio de credenciais de acesso, mesmo depois de bloqueadas.

SEÇÃO II – SENHAS

- As senhas são pessoais e intransferíveis, não podendo ser compartilhadas com outros COLABORADORES, ainda que a pedido de seu superior hierárquico, e tampouco divulgadas a terceiros, inclusive durante período de eventual afastamento de suas atividades laborativas, como licença e/ou férias.
- Os COLABORADORES do **ICL** são responsáveis pela confidencialidade das senhas associadas aos identificadores de acesso que utilizam.
- Os COLABORADORES do **ICL** são responsáveis por toda e qualquer ação realizada mediante utilização de suas credenciais de acesso.
- A senha de acesso à rede de dados do **ICL** deve ter as seguintes características:
    - Tamanho mínimo de 9 elementos alfanuméricos.
    - Deve ser modificada a cada 45 dias.
    - Não é permitida a reutilização das 10 últimas senhas.
- A reinicialização de qualquer senha associada a determinado identificador de acesso somente pode ser solicitada pelo próprio responsável por seu uso, em caráter excepcional e mediante solicitação.
- As senhas reinicializadas ou inicialmente atribuídas a identificadores de acesso devem respeitar as regras de formatação, serem aleatórias e, sempre que possível, alteradas na primeira ocasião em que forem utilizadas.
- As senhas relacionadas ao uso de Ativos de TI são automaticamente bloqueadas após cinco sucessivas tentativas fracassadas de autenticação.
- As senhas de acesso não devem ser incluídas ou salvas em programas, rotinas e procedimentos para acesso automatizado.

- As senhas de acesso destinadas à execução de programas, rotinas e procedimentos que demandem acesso automatizado aos Ativos de TI devem ser utilizadas exclusivamente para tal fim e não devem ser semelhantes a senhas utilizadas por COLABORADORES em outros ambientes e contextos alheios ao **ICL**.

CAPÍTULO VI – USO DA INTERNET

- Todos os dados que trafeguem pela rede do **ICL** estão sujeitos ao monitoramento por esta entidade.
- É expressamente proibido o uso da internet por COLABORADORES do **ICL** para acessar mensagens, fotos, vídeos, arquivos e qualquer outro similar com conteúdo obsceno, discriminatório, racista ou similares e que viole Leis, Regulamentos, Normas, Direitos, Estatuto , Regimento Interno , Política de Segurança da Informação , Código de Integridade e Conduta do **ICL**. Eventuais inadequações serão de única e exclusiva responsabilidade do COLABORADOR.
- A internet somente deve ser utilizada para exercício de atividades voltadas aos interesses institucionais do **ICL**, salvo se expressamente autorizado pelo Conselho Deliberativo ou pelo Conselho Fiscal, mas sempre observando o item anterior.
- A utilização da internet, no âmbito do **ICL**, deve ser realizada exclusivamente através da infraestrutura por ela disponibilizada e autorizada.
- Podem ser impostos limites adicionais à utilização da internet, com vistas a preservar a disponibilidade, segurança e integridade do acesso.
- O acesso a conteúdo destoante dos interesses institucionais ou que represente ameaça à segurança de ativos de informação será bloqueado.
- Todos os acessos à internet devem ser registrados e os registros que forem obtidos poderão ser utilizados para detecção de violações da Política de Segurança de Informação.
- O acesso dos COLABORADORES pode ser revogado nos casos de ameaça iminente a Ativos TI e informações ou de desrespeito à Política de Segurança de Informação.
- Os registros de acesso à internet serão regularmente analisados com o objetivo de identificar as ameaças iminentes a ativos de informação e as evidências de desrespeito à Política de Segurança da Informação.
- Os COLABORADORES devem repassar ao Conselho Fiscal qualquer conteúdo suspeito ou que represente ameaça a Ativos de TI e informações.

CAPÍTULO VII – CORREIO ELETRÔNICO (E-MAIL)

- Todo e qualquer dado transmitido ou recebido através do correio eletrônico institucional está sujeito ao monitoramento do **ICL**.
- É expressamente proibido o uso do correio eletrônico por COLABORADORES do **ICL** com mensagens, fotos, vídeos, arquivos e outros com conteúdo obsceno, discriminatório, racista ou similares e que viole Leis, Regulamentos, Normas, Direitos, Estatuto , Regimento Interno , Política de Segurança da Informação e Código de Integridade e Conduta do **ICL**. Eventuais inadequações serão de única e exclusiva responsabilidade do COLABORADOR.
- O correio eletrônico deve ser utilizado exclusivamente para o exercício das atividades institucionais do **ICL** e armazenado somente em equipamentos fixos ou móveis do **ICL**, salvo se expressamente autorizado autorizado pelo Conselho Deliberativo ou pelo Conselho Fiscal, mas sempre observando o item anterior.
- Todo COLABORADOR é integralmente responsável pelo conteúdo das mensagens enviadas através de seu endereço de e-mail.
- O endereço de correio eletrônico individual deve privilegiar a composição formada pelo primeiro nome e/ou por um sobrenome do COLABORADOR separados por um ponto (joao@combustivellegal.com.br / joao.silva@combustivellegal.com.br)
- O endereço de correio eletrônico de cada COLABORADOR é de uso individual e intransferível.

- Ao receber qualquer mensagem (incluindo os anexos) na sua Caixa de Correio Eletrônico, o COLABORADOR deve buscar ter ciência de quem é o remetente.
- Mensagens enviadas para endereços externos devem incluir, ao final de seu corpo, aviso padrão sobre a sua confidencialidade e sobre a exclusividade de utilização de seu conteúdo pelos destinatários legítimos (procedimento automático).
- É vedado o envio ou troca de mensagens contendo diversos destinatários externos (*mailing list*). Deverá ser dada elevada preferência ao envio de e-mails individuais, ou seja, a apenas um destinatário externo. Caso seja necessário o envio para múltiplos destinatários externos, o endereço de e-mail de cada destinatário deverá ser inserido em cópia oculta no e-mail.
- O sistema de correio incluirá a assinatura eletrônica com base nos dados cadastrais do **ICL**.
- Arquivos executáveis, mesmo compactados, não devem ser transmitidos em anexos a mensagens de correio eletrônico.
- O tamanho máximo do(s) arquivo(s) (compactados ou não) permitido para envio é de 20 MB.
- Os endereços de correio eletrônico de COLABORADORES devem ser bloqueados em casos de desligamento.
- O acesso dos COLABORADORES ao correio eletrônico pode ser revogado temporária ou permanentemente nos casos de desrespeito à Política de Segurança da Informação, violação ao Código de Integridade e Conduta ou ameaça aos Ativos de TI ou às informações do **ICL**.
- A transmissão ou a recepção, no correio eletrônico, de conteúdo dissonante dos interesses institucionais ou que seja potencialmente danoso à segurança dos Ativos de TI ou informações será bloqueada pelo **ICL**, sem prejuízo da adoção de outras medidas cabíveis.
- Limites adicionais à utilização do correio eletrônico podem ser impostos, a critério do **ICL**, com vistas a preservar a disponibilidade, segurança e integridade do ambiente de TI.

CAPÍTULO VIII – APLICATIVOS DE MENSAGENS

- Todo e qualquer dado transmitido ou recebido através do aplicativos de mensagens instalados nos equipamentos fixos e móveis do **ICL** está sujeito ao monitoramento pelo **ICL**.
- É expressamente proibido o recebimento e envio de mensagens, fotos, vídeos, arquivos e qualquer outro similar por COLABORADORES do **ICL** com conteúdo obsceno, discriminatório, racista ou similares e que viole Leis, Regulamentos, Normas, Direitos, Estatuto , Regimento Interno , Política de Segurança da Informação e do Código de Integridade e Conduta do **ICL**. Eventuais inadequações serão de única e exclusiva responsabilidade do COLABORADOR.
- Não é permitida a participação de COLABORADORES e TERCEIROS em grupos de aplicativos de mensagens e de mensagens instantâneas para recebimento e transmissão de informações de conteúdo institucional do **ICL** e em nome do **ICL** nos equipamentos fixos e móveis do ICL e particulares, salvo se expressamente autorizado pelo Conselho Deliberativo ou pelo Conselho Fiscal, mas sempre observando o segundo item.
- Todo COLABORADOR e TERCEIRO é integralmente responsável pelo conteúdo das mensagens enviadas.
- A utilização de aplicativos de mensagens dos COLABORADORES pode ser revogado temporária ou permanentemente caso o **ICL** tenha conhecimento de desrespeito à Política de Segurança da Informação, violação ao Código de Integridade e Conduta ou ameaça aos Ativos de TI ou às informações do **ICL**, sem prejuízo das demais medidas cabíveis.
- Limites adicionais à utilização de aplicativos de mensagens podem ser impostos, a critério do **ICL**, com vistas a preservar a segurança e integridade das informações.

CAPÍTULO IX – USO E ADMINISTRAÇÃO DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

- Todo e qualquer dado transmitido, recebido ou armazenado nos Ativos de TI está sujeito ao monitoramento pelo **ICL**.

- É expressamente proibida a utilização dos Ativos de TI para acesso a mensagens, fotos, vídeos, arquivos e qualquer outro similar por COLABORADORES do **ICL** com conteúdo obsceno, discriminatório, racista ou similares e que viole Leis, Regulamentos, Normas, Direitos, Estatuto , Regimento Interno , Política de Segurança da Informação e do Código de Integridade e Conduta do **ICL**. Eventuais inadequações serão de única e exclusiva responsabilidade do COLABORADOR.
- Todos são responsáveis por zelar pela segurança dos Ativos de TI do **ICL** e devem utilizá-los somente para o exercício das atividades profissionais voltadas aos interesses institucionais.
- Os Ativos de TI devem ser inventariados periodicamente e ter seus responsáveis identificados.
- Devem ser observadas as as recomendações do fabricante para proteger os Ativos de TI de propriedade do **ICL**.
- A utilização dos Ativos de TI deve ser precedida do aceite formal dos Termos de Responsabilidade de Uso.
- Não é permitido adicionar, remover ou manipular os componentes físicos internos (hardware) dos Ativos de TI.
- É proibido desenvolver, manter, utilizar ou distribuir sistemas ou dispositivos não autorizados que possam capturar ou corromper informações armazenadas ou em trânsito, bem como danificar os Ativos de TI do **ICL**.
- Não é permitida a instalação de programas (software), independente do regime de licenciamento, sem o consentimento do gestor responsável.
- Todo COLABORADOR, ao se ausentar temporariamente da sua estação, deve bloquear o seu computador ou notebook. Esta ação assegura a autenticação para acesso ao equipamento somente por pessoa(s) autorizada(s).

CAPÍTULO X – ARMAZENAMENTO DE INFORMAÇÕES

- Os arquivos e informações institucionais do **ICL** devem ser armazenadas exclusivamente no Sistema **ICL**. O arquivamento deverá ser realizado de forma organizada, na pasta eletrônica de cada departamento.

CAPÍTULO XI – EQUIPAMENTOS MÓVEIS

- Objetivando facilitar a mobilidade e o fluxo de informações entre seus COLABORADORES, o **ICL** disponibiliza, a seu critério, equipamentos móveis (notebook, tablet e smartphone).
- O **ICL** permanece como o proprietário dos equipamentos cedidos aos COLABORADORES e reserva-se o direito de inspecioná-los a qualquer tempo.
- É fundamental que cada COLABORADOR utilize senhas de bloqueio automático para seu equipamento móvel.
- É proibida, sem autorização expressa do gestor responsável, a alteração da configuração dos sistemas operacionais dos equipamentos, principalmente, os referentes à segurança e à geração de logs.
- A reprodução não autorizada dos softwares instalados nos equipamentos móveis fornecidos pela instituição constituirá uso indevido do equipamento.
- É responsabilidade do COLABORADOR, no caso de furto ou roubo de um equipamento móvel fornecido pelo **ICL**, notificar imediatamente o gestor direto.

CAPÍTULO XII – IMPRESSORAS

- Para fins de economia, segurança da informação e respeito ao meio ambiente, o COLABORADOR do **ICL** deve avaliar a necessidade de imprimir o documento.
- Para concluir a impressão o usuário deve-se dirigir ao local de impressão para liberar o seu trabalho no local, evitando desta forma que outras pessoas retirem seu trabalho.
- Impressões erradas ou desnecessárias devem ser descartadas pela fragmentadora de papel.
- Utilize a impressora colorida somente quando necessário e apenas para a versão final de trabalhos.

CAPÍTULO XIII– ACESSO ÀS INSTALAÇÕES

- O acesso de COLABORADORES e TERCEIROS somente será permitido após cadastro do Sistema de Controle de Acesso, que conterá nome, nº do CPF, nome da empresa, telefone

CAPÍTULO XIV– CONTROLE DE REUNIÕES

- As salas de reuniões somente poderão ser utilizadas por COLABORADORES e TERCEIROS para fins institucionais do **ICL** e dependerão de reserva efetuada e aprovada antecipadamente por um COLABORADOR.
- Em todas as reuniões deverá ter um COLABORADOR presente, salvo se autorizado pelo Presidente do Conselho Deliberativo.
- Não é permitida a utilização das salas para tratar de assuntos de interesse exclusivo dos Associados, individual ou conjuntamente, devendo-se observar as regras do Código de Integridade e Conduta.
- Toda reunião deve ser precedida de convocação efetuada por um COLABORADOR, que deverá especificar a pauta, horário e local.
- A realização de reunião utilizando o recurso *video conference call* ou *conference call* somente será possível após o COLABORADOR responsável pela reunião analisar o grau de urgência e importância do assunto a ser tratado e com expressa autorização do Presidente do Conselho Deliberativo . As pessoas que participarem da reunião por *call* devem ser relacionadas na lista de presença pelo COLABORADOR responsável pela reunião, identificando que a participação foi não presencial. Além disso, os dados do (s) participante (s) (nome, nome da empresa, telefone, e-mail) e os temas abordados na reunião devem constar em ata.