1. INTRODUÇÃO À NORMA DE RESPOSTA A SOLICITAÇÃO DE TITULARES

A METALTORK INDÚSTRIA E COMÉRCIO DE AUTOPEÇAS LTDA. inscrita no CNPJ 59.160.069/0001-25, com sede na Rua Brejuva, 400, B, Piraporinha, Diadema, SP, adiante designada como **METALTORK,** prioriza a integridade das pessoas, respeitando opiniões diferentes e investindo no desenvolvimento pessoal. Age de forma dedicada, com atitude responsável e determinação para cumprir os objetivos acordados com todos, garantindo a qualidade dos processos, produtos e serviços, sempre com bastante honestidade e melhoria contínua.

2. OBJETIVO

A segurança e a privacidade são requisitos básicos para o funcionamento METALTORK, por isso, ela assume seu compromisso com a proteção dos dados de seus Clientes, Colaboradores, Fornecedores, Visitantes, Parceiros de Negócios e qualquer pessoa que acessar o seu site e plataforma ou eventualmente enviar dados pessoais para a empresa.

Para que a METALTORK consiga honrar seu compromisso com todos e atender a Lei Geral de Proteção de Dados Pessoais, é imprescindível que você, COLABORADOR, observe rigorosamente o disposto neste código.

Contamos com sua colaboração!

3. REGRAS DE CONDUTAS DA METALTORK

3.1. APLICAÇÕES GERAIS

São expressamente vedadas aos colaboradores da METALTORK as condutas abaixo:

- Representar ou dar a impressão de representar a METALTORK quando você não estiver autorizado a fazê-lo;
- Esconder sua identidade, afirmar ser outra pessoa, ou reivindicar a representação de outra pessoa, a menos que explicitamente autorizado a fazê-lo;
- Enviar ou compartilhar arquivos internos e confidenciais para contas pessoais de e-mail, sites ou fóruns de internet ou quaisquer outros meios;

- Classificar as informações confidenciais recebidas de terceiros como 'públicas' ou transmitir, compartilhar, copiar ou fornecer acesso a tais informações, exceto quando expressamente autorizadas nos termos do acordo de confidencialidade relevante;

- Armazenar, transmitir ou tomar qualquer dado não explicitamente classificado como 'Público' para fora dos limites físicos da METALTORK como aeroporto, café ou casa ou limites lógicos, como armazenamento em nuvem não aprovados, sites de transferência de arquivos não aprovados ou quaisquer sistemas não pertencentes, controlados ou aprovados pela METALTORK sem permissão explícita da Equipe de Segurança da Informação;
- Fornecer quaisquer dados não públicos a terceiros sem controles lícitos e técnicos adequados para proteger os interesses da METALTORK e de seus funcionários, clientes e parceiros;
- Supor que potenciais ameaças à segurança serão resolvidas por conta própria ou que a equipe de segurança da METALTORK já esteja ciente do potencial problema de segurança que você tenha identificado;
- Divulgar informações relevantes sobre incidentes de segurança para terceiros internos ou externos não autorizados.

3.2. INFORMAÇÕES DIGITAIS

3.2.1. O QUE DEVE SER FEITO

- Realizar log-off do computador ao se ausentar da estação de trabalho, ainda que por curto espaço de tempo;
- Acionar o Departamento de Segurança da Informação imediatamente quando identificado qualquer tipo de bloqueio no sistema que impeça a execução das atividades para que as devidas providências sejam realizadas;
- Acionar o Departamento de Segurança da Informação imediatamente quando houver suspeitas em relação ao uso indevido das senhas para que a alteração no sistema seja realizada;
- Guardar documentos no servidor em pasta própria com senha;

- Informar imediatamente ao Encarregado de Dados, através do e-mail * se você receber informações que você não esteja autorizado a receber, ou ainda se parecerem ilegais ou inadequadas;

- Utilizar mídias sociais somente quando permitido e observar este Código de Conduta e a Política de Privacidade e, demais, procedimentos de proteção de dados da METALTORK;

- Ter cuidado com a integridade e a precisão das informações acessadas através das mídias sociais – confirmar a autenticidade antes de confiar nelas;

- Recuperar, copiar ou armazenar informações de fontes externas quando for permitido e para uso profissional. É responsabilidade do indivíduo garantir que a propriedade ou direitos autorais de tais informações seja respeitada em todas as instâncias;

- Proteger sua conta de usuário e credenciais/senha. Proteja-os da mesma forma que você protege seu pin de cartão de crédito ou cartão de débito, ou qualquer outra informação altamente confidencial; e

- Acessar somente sites da METALTORK que requeira autenticação, por exemplo, login e senha, inserindo a URL na barra do navegador, usando os marcadores do seu navegador, ou gerenciador de senhas aprovado pelo Departamento de Segurança da Informação.

3.2.2. O QUE É PROÍBIDO FAZER

- Salvar no computador ou outro meio disponível (pen drive, HD externo, celular, e-mail particular), ainda que provisoriamente, documentos da METALTORK;

- Utilizar os ativos de TI da METALTORK para qualquer atividade que não esteja associada ao desempenho de suas funções na METALTORK

- Utilizar de qualquer ativo, dados pessoais e documentos de responsabilidade da METALTORK para qualquer atividade que não seja da empresa;

- Qualquer tentativa de alterar ou burlar quaisquer controles de segurança em um sistema de TI sem autorização da equipe de Segurança da Informação;

- "Ficar quieto" se você achar que clicou em link, arquivo suspeito ou tenha inserido suas credenciais em um potencial site invasor;

- Trazer para dentro das dependências físicas da METALTORK ou conectar qualquer dispositivo "encontrado" ou não aprovado em ativo de TI da METALTORK;

• Armazenar, transmitir ou disponibilizar cópias não autorizadas de material protegido por direitos autorais usando qualquer ativo da METALTORK, por exemplo, laptop, desktop, smartphone, compartilhamento em rede, sistemas de e-mail e nuvem;

• Fazer cópias ilegais de material de direitos autorais, especificamente incluindo, mas não que não se limita a utilização de programas de softwares piratas, arquivos de música ou arquivos de vídeo;

• Executar qualquer ação, por exemplo, excluir arquivos do sistema, clicar em pop-ups, desconectar, desligar o computador etc., para tentar erradicar ou conter um suposto incidente de segurança, exceto quando explicitamente instruído pela Equipe de Segurança da Informação.

3.3. Acesso a ativos e sistemas de informação

3.3.1. A METALTORK confere a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa. As referidas contas são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;

3.3.2. Toda conta de acesso é pessoal e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso;

3.3.3. Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, como por exemplo, não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pela METALTORK, observar toda as medias de segurança dispostas neste código de conduta;

3.3.4. Usuários que têm privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia;

3.3.5. A credencial é de uso pessoal e intransferível;

3.3.6. Todas as informações acessadas, independentemente da origem, são de uso exclusivo da METALTORK não sendo permitido o compartilhamento com terceiros estranhos à atividade;

3.3.7. Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo a análise do risco gerado à METALTORK em decorrência da infração pelo Encarregado de Dados e Equipe de Segurança da Informação, sendo que a aplicação das sanções e punições serão avaliada e aplicadas pelo Departamento de Recursos Humanos e Jurídico da Empresa, conforme disposto no item 3 deste Código de Conduta.

3.4. REGRAS GERAIS: E-MAIL E COMUNICADOR INSTANTÂNEO

3.4.1. O QUE DEVE SER FEITO

• Notificar a Equipe de Segurança da Informação, ou Superior hierárquico, ou Encarregado de Dados, através do e-mail * se você receber uma mensagem de e-mail suspeita; se você tiver clicado ou inserido suas credenciais, ou acreditar que pode ser vítima de um ataque cibernético, entre em contato com a equipe de segurança imediatamente por telefone;

• Transferir para ambiente eletrônico seguro e excluir do comunicador em até 15 dias úteis, as informações e histórico de mensagens decorrentes das atividades laborais obtidas via os comunicadores instântaneos;

• Observar este Código de Conduta, Política de Privacidade e, demais, procedimentos de proteção de dados, quando a METALTORK permitir que o COLABORADOR utilize aparelho próprio e escolha o serviço de comunicador instantâneo a seu critério para tratar de assuntos relacionados à sua atividade profissional;

- Efetuar o log out após cada sessão encerrada de utilização dos comunicadores instantâneos nas configurações do aplicativo.

3.4.2. O QUE É PROÍBIDO FAZER

- Utilizar qualquer serviço de e-mail ou comunicador instantâneo que não seja o oficialmente fornecido pela METALTORK;
- Utilizar do serviço de e-mail ou comunicador instantâneo em caráter pessoal e/ou para fins que não sejam de interesse da METALTORK salvo quando expressamente permitido;
- Utilizar termos ou palavras de baixo calão na redação de mensagens;
- Enviar informação classificada como de USO INTERNO e/ou CONFIDENCIAL para endereços eletrônicos que não fazem parte do domínio corporativo da METALTORK, exceto quando expressamente autorizados;
- Inscrever o endereço de e-mail ou número de comunicador instantâneo da METALTORK em listas de distribuição e grupos de discussão que não estejam relacionadas às atividades laborais ou do interesse da organização;
- Tentar interceptar ou alterar conteúdo da mensagem de outros usuários ou terceiros;
- Disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;
- Enviar mensagens cujo conteúdo incite uso de entorpecentes (drogas), pornografia, terrorismo, práticas subversivas, violência, práticas racistas, homofóbicas, gordofóbicas, demais crimes, assim como qualquer outro que possa infringir a legislação vigente, bem como os direitos e garantias das pessoas físicas;
- Clicar em links e em e-mails que possa levar a páginas fakes que tentam fazer com que você insira suas credenciais para roubo e uso malicioso de dados por invasores;
- Produzir, transmitir ou divulgar mensagem que contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da METALTORK ou que:
- Contenha ameaças eletrônicas, como: spam, e-mail bombing, vírus de computador;
- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar quaisquer sistemas de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Contenha anexo(s) superior(es) a 30 MB para envio (interno e internet) e 30 MB para recebimento (internet)
- Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade e manipulação de cabeçalhos de e-mail. Qualquer tentativa, mesmo não consumada será tratada como um incidente de segurança da informação e estará sujeita a sanções;
- Usar uma conta de e-mail não fornecida pela METALTORK para desempenho de suas funções laborais, exceto quando explicitamente autorizado a fazê-lo por um membro sênior da Equipe de Segurança da Informação.
- Enviar e receber currículos, atestados médicos, laudos médicos ou quaisquer outros documentos relacionados à saúde de qualquer pessoa, incluindo colaboradores e seus dependentes via comunicares instantâneos.

3.5. INFORMAÇÕES FÍSICAS:

3.5.1. O QUE DEVE SER FEITO:

- Guardar agendas, documentos confidenciais e internos, cadernos ou qualquer outro material de anotação em gavetas trancadas, de modo a evitar o acesso por tercerios (internos e externos) não autorizados;
- Guardar em lugar adequado e seguro, as chaves das gavetas, armários e portas de acesso, de modo a evitar que estejam sobre a mesa ou outro local exposto;
- Utilizar máquina fragmentadora, antes de descartar documento, devendo sempre observar a Política de Retenção de Dados;

- Imprimir somente documentos estritamente necessários;
- Inserir senha de indentificação para autorizar a impressão;
- Certificar de não deixou folha impressa com informações referentes à instituição, clientes ou colaboradores na impressora;

- Retirar documentos das mesas ou outras áreas de superfície nos períodos de ausência da estação de trabalho; e
- Limpar a mesa de trabaho, guardar os documentos em gavetas ou armários fechados e desligar o computador ao final do expediente.

3.5.2. O QUE É PROÍBIDO FAZER:

- Deixar anotações, recados e lembretes à amostra sobre a mesa, ou colados em paredes, divisórias ou no monitor do computador;
- Deixar senhas anotadas em cadernos, post-it ou em quaisquer lembretes que possam ser acessíveis a terceiros;
- Deixar crachá de identificação em qualquer lugar, devendo mantê-lo sempre consigo.

3.6. UTILIZAÇÃO DE EQUIPAMENTO

3.6.1. O QUE DEVE SER FEITO

- Receber apenas equipamentos originários da equipe de Segurança da Informação da METALTORK;
- Utilizar senha em todos os celulares entregues aos colaboradores pela empresa, inclusive, no próprio aplicativo de comunicador instantâneo instalado;
- Guardar os celulares em locais fechados e trancados com chave, de modo a evitar o acesso por terceiro (internos e externos) não autorizados. Ao terminar de usá-lo ou ao final do expediente, desligá-lo;

- Utilizar os equipamentos apenas para fins da empresa, exceto quando o acesso for especificamente fornecido em dispositivos pessoais, devendo observar este Código de Conduta e Política de Privacidade e, demais, procedimentos de proteção de dados da METALTORK;

- Proteger o equipamento como se fosse seu e informar imediatamente qualquer perda ou roubo à equipe de Segurança da Informação da METALTORK;

- Utilizar apenas licenças legítimas nos softwares instalados ou armazenados nos ativos da METALTORK (laptop, desktop, smartphone, compartilhamento de rede);

- Obter autorização da equipe de Segurança da Informação, ou do Superior hierárquico ou do Encarregado de Dados, através do e-mail * antes de baixar e/ou instalar qualquer software da internet em um dispositivo fornecido pela METALTORK.

3.6.2. O QUE É PROÍBIDO FAZER

- Realizar o download ou arquivar documentos pessoais nos notebooks ou outros equipamentos disponibilizados pela METALTORK, exceto quando autorizado;

- Baixar (realizar download) de jogos e programas alheios à atividade profissional e aos interesses da METALTORK;

- Retirar o celular da METALTORK, salvo se autorizado expressamente;

- Permitir que terceiros, incluindo, mas não se limitando, colegas de trabalho, amigos, familiares, utilizem seus equipamentos para atividades não relacionadas à METALTORK;

- Deixar seus equipamentos sozinhos em locais públicos;

- Remover ou armazenar em dispositivos não aprovados, de informações de propriedade da METALTORK, sejam internas, sensíveis ou confidenciais;

- Usar equipamentos disponibilizados pela METALTORK, seja em suas dependências, seja no trabalho remoto, fora do expediente do trabalho.

3.7. CLASSIFICAÇÃO E ROTULAGEM DA INFORMAÇÃO

3.7.1. Para efeitos de classificação da informação, a METALTORK utiliza as seguintes categorias:

- **INFORMAÇÃO PÚBLICA:** é a informação de uso externo e para o público em geral. A divulgação deste tipo de informação não causa problemas METALTORK ou a seus clientes podendo ser compartilhada livremente com o público desde que seja mantida sua integridade;

- **INFORMAÇÃO DE USO INTERNO:** são informações gerais destinada exclusivamente funcionários da METALTORK, não podendo ser compartilhada com o público externo. Estas informações só podem ser compartilhadas externamente mediante autorização expressa pelo Gestor da Informação;

- **INFORMAÇÃO CONFIDENCIAL:** informação de caráter sigiloso podendo ser tratada exclusivamente por aqueles que tenham sido expressamente autorizados. Necessitam conhecê-las apenas aqueles que dependem delas para o desempenho de suas tarefas profissionais e prestação de serviços perante a METALTORK. A divulgação ou alteração não autorizada desse tipo de informação pode causar graves danos e prejuízos para a METALTORK e/ou seus clientes. Portanto, seu compartilhamento deve ser restrito e feito de maneira controlada.

3.7.2. A classificação da informação deverá ser realizada pelos gestores da informação ou colaboradores por eles designados, devendo ser observado as condutas dispostas no item **3.9** deste Código.

3.7.3. Para informações classificadas como **PÚBLICAS** poderão ser utilizadas o rótulo simples, conforme quadro do Anexo I deste Código.

3.7.4. Para informações classificadas como USO INTERNO ou CONFIDENCIAIS deverá constar no rótulo a sua classificação e, quando o acesso for limitado a um setor/departamento específico deverá ser referenciado conforme item 1.2 do Anexo I deste Código.

3.8. MANUSEIO DA INFORMAÇÃO

3.8.1. As formas como as informações da METALTORK devem ser manuseadas estão dispostas no Anexo II deste Código.

3.8.2. Documentos confidenciais em suporte físico devem ser guardados em gavetas ou armários trancados de forma a impedir o acesso de pessoas não autorizadas.

3.8.3. Em períodos de ausência da estação de trabalho, os documentos em suporte físico devem ser retirados das mesas e de outras áreas da superfície.

3.8.4. Documentos de uso interno ou confidenciais disponíveis em forma eletrônica devem ser armazenados em ambientes com acesso controlado e senhas para impedir o acesso a pessoas não autorizadas.

3.8.5. Toda não-conformidade será tratada como um incidente de segurança da informação cabendo uma análise da infração pelo Encarregado de Dados, Profissional de Segurança da Informação e Jurídico da METALTORK e aplicação das sanções e punições previstas no item 3 deste Código.

3.9. GESTOR DA INFORMAÇÃO

3.9.1. É responsabilidade dos colaboradores apontados como Gestor da Informação:

- Definir a classificação das informações sob sua responsabilidade com base nas categorias de classificação constantes deste Código, mantendo um registro atualizado dos itens classificados;
- Controlar as informações geradas em sua área de negócio e atuação;
- Revisar periodicamente a classificação das informações sob sua guarda.

4. SANÇÕES E PUNIÇÕES

A inobservância de qualquer disposição deste Código de Conduta implicará nas penalidades previstas no contrato de trabalho e das medidas administrativas cabíveis, como advertência, suspensão ou dispensa por justa causa com base no artigo 482 da Consolidação das Leis do Trabalho (CLT), sem prejuízo das sanções dispostas na Política de Privacidade.

5. Gestão do Documento

5.1. O presente Documento é aprovado pelo Comitê Gestor de Privacidade e Segurança da Informação e Diretoria da METALTORK.

5.2. Este Código poderá ser revisado com periodicidade anual ou conforme o entendimento do Encarregado de Dados e Departamento de Segurança da Informação.

6. REVISÃO

- **00:** Emissão Inicial.

ANEXO I – MODELOS PARA ROTULAGEM DE INFORMAÇÕES

Os padrões a seguir representam os rótulos aprovados que devem ser exibidos nos cabeçalhos e/ou rodapés dos documentos que contenham dados pessoais, conforme nível de classificação.

Observação: A cor, fonte e tamanho do texto podem ser ajustados desde que mantida a clareza e objetividade da informação.

Responsável:	**Aprovador:**
Gabriel Amaral – Supervisor de TI	Charles Anderle – Gerente de TI

1.1. CABEÇALHO

NÍVEL	RÓTULO
INFORMAÇÃO PÚBLICA	P
INFORMAÇÃO INTERNA	I
INFORMAÇÃO CONFIDENCIAL/RESTRITA	C/R

Tabela 1. Cabeçalho.

1.2. Rodapé

METALTORK – [INSERIR NÍVEL DE CLASSIFICAÇÃO/SETOR]

Exemplo:

METALTORK – Informação Interna / Departamento de Recursos Humanos

2.

ANEXO II – AÇÃO X CLASSIFICAÇÃO

AÇÃO	CLASSIFICAÇÃO		
	Pública	Interna	Confidencial
Cópia / Exclusão	Sem restrições	Aprovação do Gestor da informação	Aprovação do Gestor da Informação
Transmissão em rede pública	Permitido	Permissão do Gestor da Informação e os arquivos devem contêm senhas fortes	Vedado
Transmissão em rede privada	Permitido	Aprovação do Gestor da Informação	Aprovação do Gestor da Informação. Recomendável criptografia para dados sensíveis e financeiros – acesso via VPN e/ou inserção de senhas fortes
Descarte	Lixo comum	Recomendável uso de trituradora.	Observar Política de Retenção de Dados. Aprovação do Gestor da Informação. Utilizar métodos aprovados descritos no item 4 da Política de Retenção
Compartilhamento com terceiros	Sem restrições	Aprovação do Gestor da Informação	Aprovação do Gestor da informação. Recomendável criptografia – aceso via VPN – Utilizar senhas fortes de desbloqueio dos documento. Assinar Termo de Tratamento de Dados com o Terceiro.
Solicitação de direitos de acesso	Sem restrições	Sem restrições	Aprovação do Gestor da Informação
Correio interno e externo	Envelope comum	Envelope comum	Identificação do destinatário específico apenas no interior do envelope. Na parte externa do envelope deverá conter o nome da empresa ou departamento e o

			endereço, quando aplicável
Rotulagem	Opcional	Na capa e em todas as páginas	Na capa e em todas as páginas.
Registro de Acompanhamento	Opcional	Registro de Log de acessos e atualizações dos documentos	Registros de Logs de acesso, Destinatários autorizados a manusear o documento, cópias/downloads efetuados, localização e atualização dos documentos e endereço de todos que acessaram.
Armazenamento	Opcional	Firewall, antivírus, AntiSpam e AntiMalware	Observar prazos da Política de Retenção de Dados. Gerir firewall, antivírus, AntiSpam, AntiMalware, testes de intrusão na infraestrutura interna. Manutenção de gestão de acessos. Realização de Backup diário. Dados sensíveis: Criptografia. Recomenda-se o uso de chave HMAC, CMAC, GMAC, (128 bits). Com definição de chave simétrica ou assimétrica específica para cada item.