POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

1. OBJETIVO

Esta Política estabelece diretrizes e regras que direcionam a Gestão da Segurança da Informação na MINDBEAT, subscrevendo princípios de confidencialidade, integridade e disponibilidade das informações de sua propriedade ou sob sua custódia, para garantir a continuidade nos processos imprescindíveis, preservação e valores institucionais, e qualidade na prestação dos seus serviços.

Os usuários devem conhecer as regras para a utilização da informação de forma segura, evitando expor qualquer informação que possa prejudicar a MINDBEAT, seus empregados, clientes, fornecedores e demais parceiros de negócios.

2. APLICAÇÃO E CONSEQUÊNCIAS

Esta Política se aplica a todos os colaboradores e parceiros de negócios que representam ou trabalham em nome da MINDBEAT.

O descumprimento dos itens descritos nesta **Política de Segurança da Informação** e nas Políticas técnicas correlatas será considerado ato infracional de indisciplina, sujeito a penalizações administrativas internas e a penalizações previstas na legislação vigente.

As penalizações podem variar de acordo com a gravidade do ato infracional, ficando os infratores sujeitos às seguintes penalidades:

- ✓ Advertência verbal;
- ✓ Advertência por escrito;
- ✓ Suspensão das atividades;
- ✓ Rescisão do contrato de prestação de serviços.

3. RESPONSABILIDADES

A direção tem como papel a liderança da organização, indicando as estratégias e os caminhos que deverão ser trilhados para alcançar os objetivos principais. O DPO da MINDBEAT é o responsável pela elaboração, manutenção, emissão e divulgação desta Política de Segurança da Informação, e avaliação das necessidades de criação de outras políticas, sejam diretas ou indiretamente ligadas à essa. Toda e qualquer Política da organização deve ser aprovada pela Direção antes de sua divulgação final.

Cada colaborador da MINDBEAT é responsável pelo cumprimento desta PSI.

A MINDBEAT compromete-se em revisar a PSI periodicamente, e atualizá-la sempre que necessário. Assim como, fornecer treinamentos adequados para que os colaboradores compreendam suas responsabilidades e obrigações em relação à segurança da informação.

4. DEFINIÇÕES

4.1. Informação:

Resultado de um processamento de dados que agrega conhecimento à pessoa que a recebe. A informação é um ativo essencial para os negócios de uma organização e necessita ser adequadamente protegida, independentemente do tipo de mídia em que estiver ou onde estiver.

4.2. Segurança da informação:

Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade e a confidencialidade das informações.

4.3. Incidente de segurança da informação:

Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação levando à perda de um ou mais princípios básicos da segurança: confidencialidade, integridade e disponibilidade.

4.4. Dispositivos móveis:

Equipamentos portáteis dotados de capacidade computacional, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets e pendrives.

4.5. Trabalho remoto:

Possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo, dentre outros, da infraestrutura interna, sem estar fisicamente na MINDBEAT.

4.6. Backup:

Uma cópia exata de um documento eletrônico, programa de computador ou disco, feito para fins de arquivamento ou para salvaguardar arquivos, na eventualidade de danificação ou destruição do original.

5. INFORMAÇÕES CONFIDENCIAIS

Consideram-se como confidenciais, quaisquer informações não disponíveis publicamente tais como especificações técnicas, manuais, esboços, modelos, materiais promocionais, e-mail, projetos, estudos, programas, documentações, comunicações internas, dados pessoais e outros. São responsáveis pela observância desta PSI todo e qualquer colaborador, ou parceiro de negócios da MINDBEAT.

O colaborador que receber informações confidenciais ou dados pessoais, deverá mantê-los e resguardá-los no referido caráter, bem como limitar seu acesso, controlar quaisquer cópias documentadas, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma destas informações ou dados pessoais, em hipótese alguma, podem ser repassadas para terceiros sem autorização da organização. Deve-se informar prontamente à MINDBEAT sobre qualquer uso ou revelação indevida de informações ou qualquer outra forma que caracterize o descumprimento desta PSI.

5.1. Classificação da Informação

A classificação das informações consiste na definição de níveis de proteção que cada dado, conteúdo de documentos e informações devem receber.

A classificação de informações e o conteúdo de documentos da MINDBEAT, foram definidos entre PÚBLICO, INTERNO E CONFIDENCIAL. Esta classificação deve ser aplicada após análise, de acordo com a importância e confidencialidade das informações.

A partir da análise das informações/documentos deve-se definir também o tratamento adequado para cada nível de classificação aplicada.

Depois de classificadas, as informações devem ser rotuladas. Ou seja, toda vez que uma pessoa receber um documento, e-mail ou qualquer outro dado, ela precisa saber sobre o seu nível de confidencialidade.

O rótulo de documentos da MINDBEAT é apresentado, no cabeçalho de cada página. De acordo com as informações descritas abaixo e a cor que representa cada uma delas:

INFORMAÇÃO PÚBLICA

A informação deve ser classificada como pública quando ela puder ser divulgada a todos, isto é, funcionários, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque impactos nos negócios da MINDBEAT. Apesar de uma informação pública não precisar de nenhum tipo de proteção quanto à questão do sigilo, é conveniente que usuário nenhum tenha acesso a ela, a menos que precise de tal informação para o desempenho de suas atividades.

INFORMAÇÃO INTERNA

A informação deve ser classificada como interna quando sua exposição fora do ambiente da MINDBEAT possa acarretar perdas financeiras, de imagem, de competitividade etc.

Para proteção de uma informação interna, se faz necessário, além de controles de acesso, conforme descrito no documento (PR_SGP_004-Procedimento_Controle_Acessos), controles que garantam sua integridade, pois são informações importantíssimas para as atividades do negócio. Informações internas, por exemplo, jamais podem ser armazenadas ou transmitidas via Internet sem a utilização de ferramentas seguras e, quando descartadas, devem ser tomadas as providências cabíveis para que a informação seja de fato destruída, sem chance de recuperação.

INFORMAÇÃO CONFIDENCIAL

A informação deve ser classificada como confidencial quando acessos não autorizados a ela, mesmo que por membros da própria organização, sejam capazes de trazer sérios danos aos negócios da MINDBEAT. Logo, a informação confidencial precisa ser protegida contra acessos internos e externos. São ainda mais importantes que as informações internas e por isso devem receber um grau de proteção ainda mais elevado.

Só devem ter acesso a informações confidenciais, pessoas que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado.

Classificação	Pública	Interna	Confidencial
Descrição	Toda e qualquer informação de domínio público, como as dispostas no site da organização.	Toda e qualquer informação disponível nas dependências da organização (intranet, sistema, memorandos, comunicados etc.). Só podem se tornar pública após aprovação da diretoria e do DPO	Toda e qualquer informação relacionada a projetos, dados pessoais, contratos etc.
Rotulação	Não há necessidade de Rotulação	Podem conter o termo “Interno” em seu cabeçalho ou divulgação.	Podem conter o termo ”Confidencial” em seu cabeçalho.
Exemplos	✓ Boletins informativos externos ✓ Impressões de sites públicos ✓ Política de Segurança da Informação ✓ Política de Privacidade e Proteção de Dados ✓ Política de Cookies	✓ Dados de negócios internos, por ex: Propostas de projetos Objetivos da empresa ✓ Procedimentos/Processos internos ✓ Documentos e formulários de treinamentos ✓ Templates de operação de projetos ✓ Modelos de contratos	✓ informações de colaboradores (informações pessoais, folha de pagamento) ✓ Dados de participantes de projetos, endereço de IP, Dados de Localização, biométricos etc. ✓ Contratos e/ou informações de

		✓ Infraestrutura de continuidade de negócios	acordos estabelecidos entre as partes envolvidas no negócio. ✓ Relatórios de auditorias ✓ Dados e Documentos enviados por clientes ✓ Dados e Documentos enviados por fornecedores
Armazenamento/Distribuição	Servidores internos ou públicos, armários.	Servidores internos, nuvem (Google Drive), chats internos (Whatsapp);	Servidores internos, nuvem (Google Drive), chats internos (Whatsapp).
Controle de Acesso	Sem Restrição	Obrigatório, por grupo de usuários, com liberação após aprovação da direção e do DPO.	Obrigatório, por grupo de usuários previamente definidos e com liberação da direção e DPO.

6. ARMAZENAMENTO DE INFORMAÇÕES

As informações serão armazenadas por um período não superior ao necessário para a realização das finalidades. Ou conforme prazo estabelecido em contrato. Após o término do período de armazenamento ou se estabelecido em contrato, as informações poderão ser excluídas ou devolvidas.

Todos os tipos de arquivos imprescindíveis para as atividades da MINDBEAT são trabalhados e armazenados em plataformas seguras, utilizadas pela companhia e por seus clientes, como por exemplo o Google Drive, Microsoft Teams e Trello.

Estas plataformas possuem além da possibilidade de armazenamento de arquivos, a edição colaborativa de documentos como Planilhas, Textos, Apresentações etc.

7. CONTROLE DE ACESSOS

Os acessos à infraestrutura interna da MINDBEAT e aos sistemas utilizados pela empresa são permitidos apenas mediante identificação e autenticação do usuário (Login), os quais terão acesso restrito ao que lhes é autorizado.

O acesso será concedido mediante avaliação prévia, e de acordo com critérios estabelecidos pela empresa, e descritos no documento (Procedimento de Senhas e Controle de Acessos), como por exemplo, a função do usuário, atividades que deverá desempenhar, e informações necessárias para realização de suas atividades.

7.1. Senhas

A MINDBEAT determina a elaboração e utilização de senhas individuais para os usuários de seus sistemas e serviços.

As senhas para utilização de sistemas e serviços devem obedecer aos critérios estabelecidos pela MINDBEAT, conforme descrito no documento (Procedimento de Senha e Controle de Acessos).

Nenhum colaborador, em hipótese alguma, deverá solicitar e/ou manter sua senha anotada em papel, post-it ou outro meio.

Nenhum colaborador está autorizado a informar sua senha para terceiros, mesmo em casos de ausência e necessidade de acesso a determinado arquivo, software ou serviço.

7.2. Acesso a E-mails

A MINDBEAT disponibiliza e-mails corporativos para todos os colaboradores da organização, e/ou parceiros que trabalham em nome da MINDBEAT, assim que são integrados à organização.

A equipe de T.I da MINDBEAT é responsável pelas contas desde a criação até sua eventual remoção, além de auditorias.

7.3. Aplicativos e Plataformas

O acesso a aplicativos e plataformas utilizadas pela MINDBEAT será concedido pela empresa após análise da direção. Para acessá-los será necessário a criação de um usuário e senha individuais e apropriados, de acordo com os critérios estabelecidos no Procedimento de Senhas e Controles de Acesso.

7.4. Informações da empresa

As informações da empresa devem ser classificadas de acordo com o item 5.1 deste documento, e só devem ser acessadas por usuários elegíveis aos critérios de classificação.

Caso o usuário ainda não possua acesso às informações, e necessite acessá-las, este deverá solicitar acesso à (TI ou Direção?) para que o acesso seja analisado e concedido posteriormente.

7.5. Documentos e informações de projetos

Documentos e informações de projetos devem ter seu acesso restrito, conforme os critérios de classificação do item 5.1 deste documento, e só devem ser acessadas por usuários que necessitem destas informações/documentos para execução das atividades relacionadas ao projeto em questão.

Caso o usuário ainda não possua acesso às informações, e necessite acessá-las, este deverá solicitar acesso à (TI ou Direção?) para que o acesso seja analisado e concedido posteriormente.

8. TRANSFERÊNCIA DE INFORMAÇÕES

O compartilhamento de informações ou dados pessoais será realizado apenas quando necessário para a realização das finalidades das atividades praticadas pela MINDBEAT. O compartilhamento de informações ou dados será informado aos envolvidos, e medidas adequadas serão adotadas para garantir a segurança das informações e dos dados pessoais compartilhados, incluindo a celebração de acordos que prevejam o compartilhamento adequado, a segurança e proteção das informações e dados pessoais, além da conformidade com as leis de proteção de dados pessoais aplicáveis.

Para a troca de arquivos entre colaboradores, a MINDBEAT disponibiliza um serviço de armazenamento compartilhado através do Google Drive. Os arquivos compartilhados internamente devem ser inseridos na pasta/local designado à informação e sinalizado ao destinatário para que possa acessá-lo.

8.1. Transferência por E-mails

Grande parte da comunicação diária da MINDBEAT se dá por meio de e-mails, portanto algumas atenções especiais devem ser tomadas, visto que um e-mail oriundo de um cliente, parceiro ou amigo pode não ter sido enviado necessariamente por este, e ameaças podem ser disseminadas. Os itens a seguir listam pontos importantes e essenciais para um melhor uso da ferramenta:

- O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação ao destinatário;
- Desconfie de todos os e-mails com assuntos estranhos;
- Evite o envio de grande quantidade de mensagens de e-mail (SPAM) que seja prejudicial à rede ou gere reclamações de outros usuários, como por exemplo, publicidades, anúncios, propaganda política etc.
- Não encaminhe e-mails do tipo corrente;
- Esteja atento ao clicar em links no corpo do e-mail;
- Não se deve utilizar o e-mail da organização para assuntos pessoais;
- As contas de e-mail com o domínio da organização poderão passar por auditorias sem prévio aviso;
- Não é permitido má utilização da linguagem em respostas aos e-mails comerciais, como abreviações de palavras, uso de gírias etc.;
- Organize sua caixa de entrada para uma fácil recuperação dos e-mails;
- E-mails que possuam como conteúdo, detalhes de projetos, ou mesmo relacionados a projetos com alto grau de sigilo, devem ser tratados de acordo com

os critérios de classificação de informações estabelecidos nesta política, e armazenados ou enviados apenas após avaliação das informações.

- Os dados de acesso ao e-mail corporativo são liberados na integração do colaborador, e sua senha de acesso deve respeitar o Procedimento de Senhas e Controle de Acessos.
- Sempre que um e-mail possuir links para acessos externos à mensagem e o colaborador estiver em dúvida quanto a sua veracidade, deve-se solicitar ajuda ao DPO antes de qualquer ação imediata;
- Se você clicou em algum link de e-mail, que considera suspeito, comunique IMEDIATAMENTE ao DPO, mantendo o e-mail em sua caixa, sem exclui-lo;
- Nenhum dado pessoal deve ser transferido por e-mail sem o uso de criptografia;
- Não se deve obter, armazenar, utilizar ou repassar materiais de conteúdo ilegal de qualquer espécie, que quebre a privacidade de terceiros, ou que seja vulgar, obsceno, pedófilo, preconceituoso, racista, ofensivo etc.;
- É terminantemente proibido a divulgação e ou repasse de informações institucionais classificadas como interna e/ou confidencial que não estejam oficialmente autorizadas pela MINDBEAT;
- É terminantemente proibido a divulgação, repasse ou compartilhamento de dados pessoais sob controle ou operados pela MINDBEAT sem prévia autorização;
- É terminantemente proibido utilizar o serviço para transferência de arquivos pessoais e ou particulares;
- É terminantemente proibido falsificar e ou excluir quaisquer atribuições a autores, avisos legais ou outros de propriedade ou da origem ou fonte de software, quando obtido de um arquivo disponibilizado por cliente;

9. TRABALHO REMOTO

A MINDBEAT possibilita o trabalho remoto a seus colaboradores e parceiros de negócios que trabalham em nome da empresa. Porém, para esta atividade, o colaborador e/ou parceiro devem seguir as diretrizes abaixo estabelecidas nesta política, tal como as informações descritas no contrato de prestação de serviços.

9.1. Utilização de dispositivos pessoais

Os usuários devem armazenar informações e documentos relacionados à MINDBEAT ou aos projetos da MINDBEAT somente no Google Drive, Microsoft Teams e Trello, utilizados pela empresa;

O usuário deve transferir informações e/ou arquivos relacionados à MINDBEAT ou aos projetos da MINDBEAT somente através do endereço de e-mail corporativo, elaborado e fornecido pela empresa, conforme item 9.1 desta política.

Para execução das atividades relacionadas à MINDBEAT ou aos projetos da MINDBEAT, o usuário deve utilizar apenas os softwares e plataformas autorizadas pela empresa

O usuário deve manter antivírus instalado, ativo e atualizado nos dispositivos utilizados para a realização de atividades da MINDBEAT ou de projetos da MINDBEAT

O usuário deve manter uma rede de internet segura e protegida para realização de atividades da MINDBEAT ou de projetos da MINDBEAT.

10. ANTIVÍRUS

Todas as estações da MINDBEAT que utilizam como sistema operacional o Microsoft Windows, possuem um software antivírus licenciado e ativo para verificação e detecção de ameaças.

11. DISPOSITIVOS REMOVÍVEIS

Possíveis incidentes, violações e/ou vazamentos de dados devem ser comunicados ao DPO da MINDBEAT, para que sejam analisados e avaliados de acordo com os critérios estabelecidos nos procedimentos de Gestão de Riscos e Plano de Resposta e Tratamento de incidentes.

É terminantemente proibido a utilização de dispositivos de armazenamento removíveis para armazenamento de informações da MINDBEAT ou de projetos da MINDBEAT. Informações armazenadas em dispositivos removíveis serão consideradas ameaças potenciais e deverão ser eliminadas.

12. BACKUP

A MINDBEAT estabeleceu e implementou processos para armazenamento e recuperação de informações de forma segura.

Os backups são realizados em conformidade com os requisitos legais e regulamentares pelo CubeBackup, periodicamente (a cada hora).

O CubeBackup protege os dados e informações armazenados pela companhia no Google Drive e Microsoft 365, e permite a restauração dos dados e metadados incluindo permissões de acesso, rótulos de e-mails e estrutura de pastas.

13. MESA LIMPA E TELA LIMPA

Todos os colaboradores e/ou prestadores de serviços, que trabalham em nome da MINDBEAT são responsáveis pelas informações tratadas em seus postos e ambientes de trabalho, e devem garantir a segurança destes, de acordo com as diretrizes definidas e descritas pela empresa nesta política.

A diretrizes descritas nesta política devem ser consideradas, de modo que mídias removíveis, papéis e documentos sobre projetos ou dados pessoais não fiquem expostos a acessos não autorizados,

Os documentos em papéis ou salvos em mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas, preferencialmente, trancados, quando não estiverem em uso, especialmente fora do horário do expediente;

O usuário deve considerar que se não estiver utilizando a informação, esta não deve ficar exposta, reduzindo o risco de acesso não autorizado, perda e danos à informação, sendo esta dado pessoal ou não;

O ambiente dos departamentos e ou áreas de trabalho (quando em ambientes home office), devem ser mantidos limpos, devendo-se atentar aos copos com líquidos (canecas e copos) e ou alimentos pela sua mesa de trabalho;

Agendas, livros ou qualquer material que possam ter informações sobre a instituição ou informações particulares devem sempre ser guardadas em locais fechados, evitando o acesso não autorizado, bem como chaves de gavetas, armários e de portas de acesso;

Ao se ausentar, deixe a tela da sua estação bloqueada a fim de evitar que outras pessoas possam ter acesso às informações não destinadas a elas. O sistema automaticamente bloqueia as telas após 5 minutos.

ATENÇÃO: Todas essas regras devem ser respeitas inclusive pelos colaboradores em Home Office, pois seu ambiente local de trabalho acaba se tornando uma extensão da MINDBEAT.

14. TRATAMENTO DE INCIDENTES

Todo e qualquer incidente de segurança da informação deve ser obrigatoriamente registrado através do documento FO_SGP_001_Formulário de Registro de Incidentes de Segurança e informado, pelo usuário, ao DPO da MINDBEAT através do canal disponibilizado pela empresa (email: dpo@mindbeat.co) quando tomarem conhecimento do incidente.

Este processo deve respeitar as diretrizes definidas e estabelecidas pela empresa no documento: PR_SGP_001_Procedimento_Plano de Resposta e Tratamento de Incidentes.

15. DISPOSIÇÕES FINAIS

Esta Política de Segurança da Informação será revisada periodicamente para garantir a sua conformidade com leis e normas aplicáveis. Alterações serão informadas aos envolvidos, quando necessário.

16. HISTÓRICO DE REVISÕES

Revisão	Data	Itens revistos	Responsável pela revisão	Aprovação
00	20/09/2024	Elaboração da Política		André Carvalho

_____

André Monteiro – Founder MINDBEAT