

1. Visão Geral

O uso aceitável, no que se refere à Taboola.com Ltd., suas subsidiárias e afiliadas (em conjunto, "Taboola" ou "Sociedade"), é uma declaração das diretrizes criadas com o objetivo de definir as práticas adequadas relativas ao uso dos recursos tecnológicos da Taboola. Esses recursos podem incluir, mas não se limitam a(o), (i) uso da Internet, computadores, dispositivos móveis, dispositivos de impressão e plataformas de comunicação eletrônica, como e-mail e mídias sociais; (ii) segurança de dados; e (iii) confidencialidade. Esta política também descreve as sanções e medidas que podem ser tomadas caso as regras aqui contidas sejam violadas.

As intenções da Taboola em publicar uma política que reúne as referidas diretrizes e sanções (doravante denominada "Política de Uso Aceitável") não são de impor restrições contrárias à cultura estabelecida da Taboola de abertura, confiança e integridade. A Taboola está comprometida em proteger seus colaboradores, parceiros e a Sociedade de ato ilegais ou prejudiciais causados por indivíduos, de forma consciente ou inconsciente.

2. Objetivo

O objetivo desta política é descrever o uso aceitável de equipamentos de informática e tecnologia da informação ("TI") na Taboola. Estas regras existem para proteger todas as pessoas que trabalham na ou em nome da Taboola. O uso inadequado expõe a Taboola a riscos, incluindo ataques de vírus, comprometimento de sistemas e serviços de rede, e questões legais.

Segurança eficaz é um esforço de equipe que envolve a participação e suporte de todos os colaboradores e afiliados da Taboola que lidam com informações e/ou sistemas de informação. É responsabilidade de todo usuário conhecer estas diretrizes e conduzir suas atividades em conformidade com elas.

3. Escopo

Esta Política de Uso Aceitável se refere à segurança e uso de todas as informações e equipamentos de TI da Taboola. Também inclui diretrizes sobre o uso do e-mail, Internet, equipamentos de TI móveis e de voz, mídia de armazenamento e pastas compartilhadas em rede, incluindo quando acessados em dispositivos pessoais que você opte por utilizar para trabalhar (quando autorizado pela Taboola). Esses sistemas devem ser utilizados para fins comerciais, atendendo aos interesses da Sociedade, e dos nossos clientes no curso normal de operações.

Esta política se aplica a qualquer indivíduo/pessoa que seja colaborador da Taboola, contratado que forneça serviços à Taboola e/ou qualquer um de seus colaboradores ou qualquer pessoa que atue em nome de tais contratados, ou qualquer preposto que atue em nome da Taboola (doravante: "você" ou "Usuário(s)"). Esta política se aplica a todas as informações, sob qualquer forma, relacionadas às atividades comerciais da Taboola em todo o mundo, e a todas as informações tratadas pela Taboola, além de cobrir todas as estruturas de TI operadas pela Taboola ou em seu nome.

4. Política

a. Uso Geral e Propriedade

- i) Todas as informações proprietárias da Taboola armazenadas em dispositivos eletrônicos e de informática, pertencentes a ou locados pela Taboola, colaborador ou terceiro, permanecem propriedade exclusiva da Taboola. Você deve garantir, por meios legais ou técnicos, que as informações proprietárias estejam protegidas de acordo com as Políticas Internas de TI.
- ii) Você tem a responsabilidade de relatar imediatamente qualquer furto ou potencial furto, perda ou revelação não autorizada de informações proprietárias da Taboola.
- iii) Você pode acessar, utilizar ou compartilhar informações proprietárias da Taboola apenas na medida em que isso seja autorizado e necessário para realizar seu trabalho.
- iv) Você é responsável por exercer o seu bom senso em relação ao uso pessoal de sistemas de TI, como dispositivos, software, contas SaaS ou serviços em nuvem. As diretrizes sobre o uso pessoal dos sistemas de TI da Taboola podem ser encontradas no espaço interno das políticas de TI (Brain), disponíveis em <https://brain.taboola.com/display/IITP> ou na pasta compartilhada do Google Drive, disponível em <https://drive.google.com/drive/u/0/folders/0ANEYIs9LeB0eUk9PVA> ("Políticas Internas de TI"). Se houver alguma incerteza, consulte seu supervisor ou gerente.
- v) Para fins de segurança e manutenção de rede, indivíduos autorizados na Taboola podem monitorar equipamentos, sistemas e tráfego de rede a qualquer momento, conforme as Políticas Internas de TI da Taboola, incluindo quando acessados em dispositivos pessoais que você opte por utilizar para trabalhar (quando autorizado pela Taboola).
- vi) A Taboola reserva-se o direito de auditar redes e sistemas periodicamente para garantir o cumprimento desta política.

b. Segurança e Informações Proprietárias

- i) As senhas do sistema e dos usuários devem estar em conformidade com as Políticas Internas de TI. É proibido fornecer acesso a outro indivíduo, deliberadamente ou por falha em proteger o acesso.
- ii) Todos os dispositivos de informática pertencentes à Sociedade e dispositivos pessoais que você opte por utilizar para trabalhar (quando autorizado pela Taboola) devem ser protegidos por um sistema MDM ("*Mobile Device Management*"). O MDM permite que o TI controle os laptops e telefones pertencentes à Taboola remotamente, controle a criptografia do dispositivo, limpe remotamente o dispositivo (se necessário) e aplique a política de proteção e de senhas da organização em cada dispositivo.

- iii) Todos os dispositivos de informática devem ser protegidos com um protetor de tela resguardado por senha, com o recurso de ativação automática definido para 15 minutos ou menos. Você deve bloquear a tela ou fazer logoff quando o dispositivo estiver sem vigilância.
- iv) As postagens de colaboradores ou contratados autorizados e terceiros a partir de um endereço de e-mail da Taboola em grupos de notícias, redes profissionais ou sites de mídia social devem ser estritamente profissionais e incluir apenas os fatos necessários, sem nenhuma opinião pessoal, agenda política, informações de clientes ou informações pessoais, e estarão sujeitas à Política de Mídia Social da Taboola, disponível em <https://www.taboola.com/pdf/social-media-policy> ("Política de Mídia Social").
- v) É necessário extremo cuidado ao abrir anexos dos e-mails recebidos de remetentes desconhecidos, que podem conter *malware*. Quando em dúvida, você deve encaminhar o e-mail para security@taboola.com.

c. Uso Inaceitável

As atividades a seguir são, em geral, proibidas. Alguns dos Usuários podem estar isentos dessas restrições durante o curso de suas responsabilidades profissionais legítimas (por exemplo, a equipe de administração de sistemas pode precisar desativar o acesso à rede de um *host* se esse *host* estiver interrompendo os serviços de produção).

Em nenhuma circunstância um colaborador da Taboola está autorizado a se envolver em qualquer atividade ilegal sob as leis locais, estaduais, federais ou internacionais enquanto utiliza os recursos de propriedade da Taboola.

As listas abaixo não são, de forma alguma, exaustivas, mas buscam fornecer um enquadramento para atividades que se classificam como uso inaceitável.

i) Atividades no Sistema e na Rede

As atividades a seguir são estritamente proibidas:

- (1) Violação dos direitos de qualquer pessoa ou sociedade que sejam protegidos por direitos autorais, segredo comercial, patente ou outra propriedade intelectual, ou leis ou regulamentos semelhantes, incluindo, entre outros, a instalação ou distribuição de software "pirateado" ou outros produtos que não estejam devidamente licenciados para uso pela Taboola.
- (2) Cópia não autorizada de materiais protegidos por direitos autorais ou confidenciais, incluindo, mas não limitado a, dados provenientes de bancos de dados, dados provenientes de servidores, arquivos de log, digitalização e distribuição de fotografias de revistas, livros ou outras fontes protegidas por direitos autorais, músicas protegidas por direitos autorais e instalação de qualquer software protegido por direitos autorais para o qual a Taboola ou o usuário final não possua uma licença ativa.
- (3) Acessar o computador ou sistema, software ou dados de qualquer pessoa sem seu conhecimento e consentimento; violar a segurança de outro usuário; ou tentar burlar a autenticação do usuário ou segurança de qualquer host, rede ou

conta. Isso inclui, mas não se limita, ao acesso não autorizado a dados confidenciais, login em ou uso de um servidor ou conta que você não esteja expressamente autorizado a acessar ou a investigação da segurança de outros *hosts*, redes ou contas.

- (4) Acessar dados, um servidor ou uma conta para qualquer finalidade que não seja a realização de negócios relacionados à Taboola.
- (5) Exportar software, informações técnicas, software de criptografia, ou tecnologia, violando as leis internacionais ou regionais de controle de exportação. A gerência deve ser consultada antes da exportação de qualquer material que esteja em questão.
- (6) Introdução de programas maliciosos na rede ou no servidor (por exemplo, vírus, *worms*, cavalos de Tróia, "bombas de e-mail", etc.).
- (7) Revelar a senha da sua conta a outros ou permitir o uso da sua conta por outros. Isso inclui família e outros membros do agregado familiar.
- (8) Usar um dispositivo Taboola para se envolver ativamente na aquisição ou transmissão de material que viole leis sobre assédio sexual ou sobre hostilidade no local de trabalho na jurisdição local do usuário.
- (9) Fazer ofertas fraudulentas de produtos, itens ou serviços com origem de qualquer conta da Taboola.
- (10) Fazer declarações sobre garantia, expressa ou implícita, a menos que faça parte das tarefas normais do trabalho.
- (11) Efetuar violações de segurança ou interrupções na comunicação da rede. Violações de segurança incluem, mas não se limitam, ao acesso a dados dos quais o Usuário não seja um destinatário pretendido ou o login em um servidor ou conta que o Usuário não esteja expressamente autorizado a acessar, a menos que essas tarefas estejam dentro do escopo de tarefas regulares. Para os fins desta seção, "interrupção" inclui, mas não se limita a, *sniffing* de rede, *ping floods*, falsificação de pacotes (*packet spoofing*), negação de serviço e informações de roteamento forjadas para fins maliciosos.
- (12) Varreduras de portas ou de segurança são expressamente proibidas, a menos que seja feita uma notificação prévia à Taboola.
- (13) Realizar qualquer forma de monitoramento de rede que intercepte dados não destinados ao *host* do Usuário, a menos que essa atividade faça parte do trabalho/dever normal do Usuário.
- (14) Burlar a autenticação do usuário ou a segurança de qualquer *host*, rede ou conta.
- (15) Introdução de *honeypots*, *honeynets* ou tecnologia similar na rede Taboola.
- (16) Interferir ou negar serviço a qualquer usuário que não seja o *host* do Usuário (por exemplo, ataque de negação de serviço).

(17) Utilizar qualquer programa/*script*/comando ou enviar mensagens de qualquer tipo com a intenção de interferir com ou desativar a sessão do terminal do usuário, por qualquer meio, localmente ou via Internet/Intranet/Extranet.

(18) Fornecer informações sobre, ou lista dos, colaboradores da Taboola a terceiros fora da Taboola, sem a aprovação prévia do Diretor de Segurança da Taboola.

ii) E-mail e Atividades de Comunicação

Os endereços de e-mail da Taboola devem ser usados, principalmente, para negócios e atividades relacionadas à Taboola. Os endereços de e-mail da Taboola não devem ser usados em conjunto com serviços pessoais.

E-mails pessoais ou comunicações (como Whatsapp, Telegram, e outros) não devem ser utilizados para comunicações de trabalho.

Ao usar os recursos da Sociedade para acessar e usar a Internet, os usuários devem perceber que representam a Sociedade. Sempre que os Usuários se afirmem como afiliados à Sociedade, eles deverão ser estritamente profissionais e deverão incluir apenas os fatos necessários, sem nenhuma opinião pessoal, agenda política, informações de clientes ou informações pessoais.

As seguintes atividades são proibidas:

(1) Envio de e-mails não solicitados, incluindo o envio de "lixo eletrônico" ou outro material publicitário a indivíduos que não solicitaram especificamente esse material (spam por e-mail).

(2) Qualquer forma de assédio via e-mail ou telefone. O assédio inclui o envio de mensagens que contenham linguagem profana ou ofensiva, o envio frequente de mensagens não solicitadas ou o envio de mensagens extremamente longas.

(3) Uso não autorizado ou falsificação de informações de cabeçalho de e-mail.

(4) Solicitação de e-mail para qualquer outro endereço de e-mail que não aquele da conta da pessoa que o postou, com a intenção de assediar ou coletar respostas.

(5) Criação ou encaminhamento de "correntes", "Ponzi" ou outros esquemas de "pirâmide" de qualquer tipo.

(6) Uso de e-mail não solicitado originado das redes da Taboola de outros provedores de serviços de Intranet/Extranet em nome de ou para anunciar qualquer serviço hospedado pela Taboola ou conectado via rede da Taboola.

(7) Postagem das mesmas mensagens ou de mensagens similares não relacionadas aos negócios para um grande número de grupos de notícias da Usenet (spam de grupos de notícias), fóruns on-line ou plataformas de discussão na internet – a menos que previamente aprovado pela Sociedade.

iii) Blogs e Mídias Sociais

- (1) Os blogs de colaboradores ou contratados autorizados e terceiros, que utilizam os bens e sistemas da Taboola ou sistemas de computadores pessoais, também estão sujeitos aos termos e restrições estabelecidos nesta Política de Uso Aceitável. O uso limitado e ocasional dos sistemas da Taboola para participar de blogs é aceitável, desde que seja feito de maneira profissional e responsável, não violando nenhuma das políticas da Taboola (incluindo, mas não se limitando à, Política de Mídia Social da Taboola), não prejudicando os interesses da Taboola, e não interferindo com os deveres regulares de trabalho dos Usuários.
- (2) As Políticas Internas de TI da Taboola relativas a informações confidenciais também se aplicam aos blogs. Assim, os Usuários são proibidos de revelar qualquer informação confidencial ou proprietária da Taboola, segredos comerciais ou qualquer outro material coberto por qualquer uma das políticas da Taboola.
- (3) Os Usuários não devem desenvolver nenhuma atividade de blog que possa prejudicar ou manchar a imagem, reputação e/ou *goodwill* da Taboola e/ou de qualquer de seus colaboradores. Os Usuários também são proibidos de fazer comentários discriminatórios, depreciativos, difamatórios ou ofensivos ao blogar ou de se envolver em qualquer conduta proibida por qualquer uma das Políticas Internas de TI da Taboola e pela Política de Mídia Social da Taboola.
- (4) Os Usuários também não podem atribuir declarações, opiniões ou crenças pessoais à Taboola quando envolvidos em atividades de blogs. Se um Usuário estiver expressando suas crenças e/ou opiniões em blogs, o Usuário não poderá, expressa ou implicitamente, se apresentar como colaborador ou representante da Taboola. Os Usuários assumem todo e qualquer risco associado às atividades de blogs.
- (5) Além de seguir todas as legislações referentes ao manuseio e revelação de materiais protegidos por direitos autorais ou sujeitos a controle de exportação, as marcas registradas, os logotipos e qualquer outra propriedade intelectual da Taboola também não poderão ser utilizados em conexão com qualquer atividade de blog.

5. Observância da Política

i) Verificação de Cumprimento

A Taboola verificará o cumprimento desta política por meio de vários métodos, incluindo, mas não se limitando a, relatórios de ferramentas de negócios, auditorias internas e externas, e feedback ao proprietário da política.

ii) Exceções

Qualquer exceção à política deve ser aprovada previamente pela Taboola.

iii) Não Cumprimento

O colaborador que violar esta política pode estar sujeito a ações disciplinares, inclusive demissão, conforme legislação trabalhista aplicável, não obstante o direito da Taboola de buscar indenização caso suas ações ou omissões resultem em perdas para a Taboola. Não obstante os direitos da Taboola, a violação desta política por um contratado ou por

terceiros constituirá uma violação material do contrato com a Taboola e permitirá que a Taboola rescinda imediatamente a relação com esse contratado ou terceiro.

6. Definições e Termos

As seguintes definições e termos podem ser encontrados no Glossário SANS, localizado em:

<https://www.sans.org/security-resources/glossary-of-terms/>

- a) Blog
- b) Honeypot
- c) Honeynet
- d) Informações Proprietárias
- e) Spam

7. Histórico de Revisão

Data da Alteração	Responsável	Resumo das alterações
18 de dezembro de 2019	Ariel Pisetzky	Revisão anual e implementação de informações sobre o sistema MDM.
29 de janeiro de 2020	Ariel Pisetzky	Correções ortográficas
17 de fevereiro de 2020	Jurídico & Ariel Pisetzky	Atualizações menores
23 de abril de 2020	Jurídico & Ariel Pisetzky	Pequenas atualizações & esclarecimentos sobre uso de dispositivos e comunicações pessoais
27 de outubro de 2021	Jurídico	Esclarecimento no Escopo & inclusão de referência à Política de Mídia Social da Taboola
25 de outubro de 2023	Segurança	Pequenas atualizações e links atualizados

Nome: _____

Assinatura: _____

Data: _____