



Política de Uso Aceitável

Controle do Documento

Campo	Descrição
Título	Política de Uso Aceitável
Código do Documento	ZDT-PUA-001
Versão	1.0
Data de Criação	26/04/2026
Última Revisão	26/04/2026
Próxima Revisão	26/04/2027
Responsável	Diretoria
Classificação	Interno
Aprovado por	Diretoria ZanderTek

Histórico de Revisões

Versão	Data	Descrição	Responsável
1.0	26/04/2026	Criação inicial da política	Diretoria

Sumário

1.	OBJETIVO.....	4
2.	ESCOPO.....	4
3.	PRINCÍPIOS DE USO.....	4
4.	USO DE E-MAIL E COMUNICAÇÃO	4
5.	USO DE INTERNET E SISTEMAS	4
6.	USO DE APLICAÇÕES E SERVIÇOS EXTERNOS	4
7.	USO DE APLICAÇÕES DE MENSAGERIA (WHATSAPP E SIMILARES).....	5
8.	USO DE DISPOSITIVOS	5
9.	PROTEÇÃO DE CREDENCIAIS.....	5
10.	USO DE INTELIGÊNCIA ARTIFICIAL	5
11.	ATIVIDADES PROIBIDAS	6
12.	MONITORAMENTO	6
13.	INTEGRAÇÃO COM OUTRAS POLÍTICAS	6
14.	RESPONSABILIDADES	6

1. OBJETIVO

Estabelecer diretrizes para o uso adequado dos recursos tecnológicos e das informações da ZanderTek, promovendo comportamento seguro, ético e alinhado aos objetivos da organização.

2. ESCOPO

Esta política aplica-se a:

- Todos os colaboradores, sócios e diretores
 - Terceiros e parceiros com acesso a sistemas ou informações
 - Todos os recursos tecnológicos utilizados pela ZanderTek
-

3. PRINCÍPIOS DE USO

Os recursos da ZanderTek devem ser utilizados de forma:

- Profissional e alinhada às atividades da organização
 - Segura, evitando exposição de riscos
 - Responsável, respeitando normas internas e externas
 - Ética, em conformidade com leis e boas práticas
-

4. USO DE E-MAIL E COMUNICAÇÃO

O e-mail corporativo deve ser utilizado de forma adequada, incluindo:

- Não enviar informações sensíveis sem proteção adequada
 - Não abrir anexos ou links suspeitos
 - Evitar uso para fins não relacionados ao negócio
 - Verificar a autenticidade de remetentes quando necessário
-

5. USO DE INTERNET E SISTEMAS

O uso da internet e dos sistemas deve:

- Estar relacionado às atividades profissionais
 - Evitar acesso a conteúdos que representem risco à segurança
 - Respeitar as diretrizes de segurança da organização
-

6. USO DE APLICAÇÕES E SERVIÇOS EXTERNOS

A utilização de aplicações externas (SaaS, plataformas online, ferramentas digitais) deve:

- Considerar o risco de exposição de informações
- Evitar o uso de ferramentas não autorizadas para dados sensíveis
- Garantir que o uso esteja alinhado às necessidades do negócio

7. USO DE APLICAÇÕES DE MENSAGERIA (WHATSAPP E SIMILARES)

A utilização de aplicações de mensageria, incluindo WhatsApp e ferramentas similares, deve observar práticas adequadas de segurança da informação.

De forma geral:

- O uso deve estar relacionado às atividades profissionais
- Deve-se evitar o compartilhamento de informações confidenciais ou sensíveis
- Informações críticas não devem ser transmitidas por esses canais sem avaliação adequada
- Deve-se ter cautela com arquivos, links e mensagens recebidas
- Sempre que possível, deve-se priorizar canais corporativos apropriados para comunicações relevantes

O uso dessas ferramentas deve considerar os riscos associados à exposição de dados e à ausência de controles formais de segurança.

8. USO DE DISPOSITIVOS

Os dispositivos utilizados devem:

- Ser utilizados de forma segura
- Estar protegidos contra acesso não autorizado
- Não ser compartilhados sem controle adequado

9. PROTEÇÃO DE CREDENCIAIS

Os usuários devem:

- Manter suas credenciais confidenciais
- Não compartilhar senhas ou acessos
- Utilizar mecanismos de autenticação segura

10. USO DE INTELIGÊNCIA ARTIFICIAL

O uso de ferramentas de Inteligência Artificial deve:

- Evitar a inserção de informações confidenciais ou restritas
- Considerar os riscos de exposição de dados
- Estar alinhado às diretrizes de segurança da organização

O uso de ferramentas de Inteligência Artificial integradas a aplicações de mensageria deve seguir as mesmas diretrizes de proteção de dados e segurança da informação.

11. ATIVIDADES PROIBIDAS

É proibido:

- Utilizar recursos da empresa para atividades ilícitas
- Compartilhar informações sem autorização
- Tentar acessar sistemas ou dados sem permissão
- Comprometer a segurança dos sistemas ou informações

12. MONITORAMENTO

O uso dos recursos tecnológicos poderá ser monitorado pela ZanderTek, respeitando os limites legais aplicáveis, com o objetivo de garantir a segurança da informação e a proteção dos ativos da organização.

13. INTEGRAÇÃO COM OUTRAS POLÍTICAS

Esta política deve ser aplicada em conjunto com:

- Política de Segurança da Informação (ZDT-PSI-001)
- Política de Proteção de Dados (ZDT-PPD-001)
- Política de Controle de Acesso (ZDT-PCA-001)

14. RESPONSABILIDADES

Colaboradores

- Utilizar os recursos de forma adequada
- Seguir esta política
- Reportar incidentes ou riscos

Diretoria

- Definir diretrizes e avaliar situações de uso indevido