Política de Permissões

Assistente LSS GB • Ambiente Microsoft Power Platform

Versão: 1.0 — minuta

Atualizada em: 25 de setembro de 2026

Status: minuta para revisão jurídica — não publicar sem aprovação.

Esta minuta define princípios, papéis e controles mínimos para conceder, revisar e revogar acessos ao Assistente LSS GB no Microsoft Copilot Studio, Teams e Microsoft 365 Copilot.

Campos entre colchetes devem ser preenchidos antes da aprovação.

1. Objetivo e abrangência

A política se aplica a usuários finais, proprietários e colaboradores do agente, administradores de ambiente e tenant, responsáveis por conectores, contas de serviço, suporte, auditoria e segurança.

Abrange o agente, seus canais, tópicos e instruções, variáveis de ambiente, conexões, fluxos, conectores, arquivos, análises, logs, relatórios, segredos, recursos vinculados e integrações com outros agentes.

2. Princípios

Menor privilégio: conceder somente o acesso mínimo necessário. Necessidade de saber: limitar dados e funções à finalidade de trabalho. Segregação de funções: separar desenvolvimento, aprovação, publicação e auditoria quando viável.

Identidade individual: evitar contas compartilhadas; usar grupos corporativos e identidades gerenciadas ou contas de serviço controladas quando tecnicamente necessário. Rastreabilidade: registrar solicitação, aprovação, alteração, revisão e revogação.

Negação por padrão: novos usuários, conectores e canais não recebem acesso até aprovação. Acesso temporário deve ter data de expiração.

3. Papéis e acessos mínimos

Usuário final — conversar com o agente, enviar apenas arquivos autorizados e baixar resultados próprios; sem editar, publicar, compartilhar ou administrar conexões.

Criador/colaborador do agente — editar componentes aprovados e testar no ambiente DEV; publicar apenas se formalmente autorizado; sem administrar o tenant ou visualizar dados sem necessidade.

Proprietário do agente — aprovar colaboradores, conexões e publicação; manter documentação, matriz de acesso e plano de continuidade; revisar permissões periodicamente.

Administrador do ambiente/Power Platform — configurar ambientes, funções, políticas DLP, capacidade, auditoria e governança; não acessar conteúdo de usuários sem finalidade administrativa legítima.

Administrador do tenant/Microsoft 365 — controlar identidades, grupos, canais, catálogo e políticas corporativas; manter separação em relação à autoria do conteúdo sempre que possível.

Responsável por conexão ou conta de serviço — manter credenciais em recurso seguro, restringir escopos e acompanhar uso; é vedado inserir segredos em prompts, variáveis abertas ou documentação pública.

Suporte/auditoria — acesso somente mediante chamado, finalidade definida, prazo e registro; preferir evidências anonimizadas ou minimizadas.

4. Matriz de referência

A matriz abaixo é um ponto de partida. Os nomes exatos das funções devem ser confirmados no tenant e no produto contratado.

Ação/Recurso	Usuário	Criador	Proprietário	Admin	Suporte/Auditoria
Conversar e enviar arquivo autorizado	Sim	Sim	Sim	Conforme necessidade	Somente em chamado
Editar tópicos, instruções e ações	Não	DEV	Sim	Não por padrão	Não
Publicar ou alterar canais	Não	Se autorizado	Sim	Apoio/controle	Não
Gerir conexões e segredos	Não	Não por padrão	Aprova	Implementa/controla	Não
Alterar variável de ambiente	Não	DEV se autorizado	Aprova	Implementa	Leitura limitada
Ler logs e transcrições	Próprios, se disponível	Só para teste autorizado	Conforme finalidade	Conforme função	Temporário e registrado
Compartilhar agente/atribuir função	Não	Não	Sim	Sim	Não

5. Solicitação e aprovação

Toda concessão deve registrar solicitante, beneficiário, função, recurso, justificativa, aprovador, data de início, validade e responsável pela implementação.

Acesso de usuário final pode seguir aprovação do gestor ou do proprietário do processo. Acesso de edição, publicação, administração, conexão ou leitura de logs requer aprovação do proprietário do agente e do responsável técnico ou de segurança definido pela organização.

Permissões emergenciais devem ser temporárias, monitoradas e revistas após o incidente.

6. Conexões, conectores e segredos

Conectores e referências de conexão devem usar identidade compatível com a finalidade, escopo mínimo e política DLP aprovada. Conexões pessoais não devem sustentar cargas de produção sem decisão formal e plano de substituição.

Segredos, tokens e chaves devem permanecer em mecanismos próprios da plataforma ou cofre aprovado. Não devem ser copiados para prompts, descrições, códigos expostos, logs desnecessários ou variáveis de ambiente legíveis por usuários não autorizados.

O conector AIROCKS – Estatísticas Green Belt e o agente de modelagem de processos somente podem receber os dados mínimos necessários à solicitação e devem ser classificados no grupo DLP adequado.

7. Ambientes e publicação

DEV deve ser usado para criação e testes com dados fictícios, anonimizados ou autorizados. Homologação e produção devem ter responsáveis, conexões e políticas próprias, evitando o reaproveitamento indevido de credenciais.

A publicação em Teams, Microsoft 365 Copilot, catálogo ou outros canais depende de testes, aprovação do proprietário, validação de segurança e confirmação de que os usuários-alvo estão corretos.

Mudanças em instruções, ações, permissões, fontes de dados, memória, autenticação ou canais devem ser avaliadas e registradas antes da promoção entre ambientes.

8. Revisão, revogação e recertificação

Permissões privilegiadas devem ser revistas ao menos trimestralmente e sempre que houver mudança de função, término de contrato, desligamento, incidente, alteração relevante do agente ou mudança de fornecedor.

O acesso deve ser revogado imediatamente quando perder a necessidade. Contas inativas, convidados, conexões órfãs e proprietários sem vínculo devem ser identificados e tratados.

A recertificação deve produzir evidência: lista de acessos, decisão do responsável, exceções, prazo de correção e confirmação de execução.

9. Monitoramento e resposta a incidentes

Eventos administrativos, falhas de conexão, publicações, alterações relevantes e acessos privilegiados devem ser monitorados conforme capacidade da plataforma e política corporativa.

Suspeitas de privilégio excessivo, credencial exposta, compartilhamento indevido ou exfiltração devem ser encaminhadas a [CANAL DE SEGURANÇA], com preservação de evidências e revogação cautelar quando proporcional ao risco.

10. Exceções e responsabilidades

Exceções exigem justificativa, análise de risco, controles compensatórios, aprovação do proprietário e da segurança, prazo definido e revisão. Exceções permanentes não são recomendadas.

Proprietário da política: [NOME/FUNÇÃO]. Aprovadores: [JURÍDICO/PRIVACIDADE], [SEGURANÇA], [NEGÓCIO]. Próxima revisão: [DATA].

Referências normativas e técnicas

Referências consultadas para esta proposta. A publicação deve considerar a versão vigente das normas, contratos e configurações do tenant.

- **Lei Geral de Proteção de Dados Pessoais — Lei nº 13.709/2018:** https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm
- **ANPD — Direitos dos titulares:** https://www.gov.br/anpd/pt-br/assuntos/titular-de-dados-1/direito-dos-titulares
- **Microsoft — Security and governance in Copilot Studio:** https://learn.microsoft.com/en-us/microsoft-copilot-studio/security-and-governance
- **Microsoft — Data loss prevention for Copilot Studio:** https://learn.microsoft.com/en-us/microsoft-copilot-studio/admin-data-loss-prevention
- **Microsoft — Configure an agent for Teams and Microsoft 365 Copilot:** https://learn.microsoft.com/en-us/microsoft-copilot-studio/publication-add-bot-to-microsoft-teams

Checklist antes da publicação

☐ Preencher razão social, CNPJ, endereço e canais de contato.

☐ Validar controlador(es), operadores, responsabilidades contratuais e fluxo real de dados.

☐ Confirmar retenção, região, memória, logs e políticas DLP efetivamente configurados.

☐ Aprovar o texto com Jurídico, Privacidade, Segurança e proprietário do produto.

☐ Mapear grupos e funções reais do tenant.

☐ Definir aprovadores, periodicidade de recertificação e canal de incidentes.

Registro de aprovação

Proprietário da política	[NOME/FUNÇÃO]
Jurídico/Privacidade	[NOME • DECISÃO • DATA]
Segurança da Informação	[NOME • DECISÃO • DATA]
Responsável de Negócio	[NOME • DECISÃO • DATA]
Data de entrada em vigor	[DATA]
Próxima revisão	[DATA]