

Before AI gets agency access

A blank working record for your team and IT provider. Use fictional records for tests. Leave out customer information, passwords and other secrets.

Tool / workflow: _____ Owner: _____

Reviewed on: _____ Provider / connector: _____

READ Which specific mailboxes, folders and records are allowed?

SEND Draft only or send? Which recipients/actions need whose approval?

CHANGE Which updates are allowed? Which changes require a human?

DISCLOSE Which providers/recipients receive data? Check terms, logs and retention.

TEST THE BOUNDARY

Try a normal request, then fictional outside text asking for an unapproved send or change. Compare the expected action with what actually happens.

Expected action / approval:

Observed result / evidence reference:

Status: verified / gap found / not verified. Open issue owner / next action:

STOP / REVOKE

Who can disable the connection, and where? _____

Guide and sources: cirlet.com/security-ai-agents