Security checklist

Nolan Ralls, founder · nolanralls.com

☑ Done: in the app today ☐ Done before anyone at the firm uses it ⬚ Planned

HOW THE APP HANDLES DATA

- ☑ **Everything runs on the PC**
  Reading, task detection and learning all happen locally. No cloud processing.
- ☑ **Read-only mail access**
  Cannot send, delete, move or change any email.
- ☑ **Encrypted storage**
  AES-256 encryption; the key is held in Windows Credential Manager.
- ☑ **One-click delete**
  Erases all local data and the saved sign-in. IT can also revoke access for everyone.
- ☑ **No outside AI**
  No ChatGPT or other AI service. The model ships inside the app.
- ☑ **Microsoft sign-in, no passwords**
  People sign in on Microsoft's own page. Your admin approves the app first.
- ☑ **Signed updates**
  The app refuses any update not signed with the publisher's key.

BEFORE THE PILOT

- ☐ **Registered company**
  Georgia LLC with its own domain and business email.
- ☐ **Signed Windows installer**
  Identity-checked signature through Microsoft. IT can push it through Intune.
- ☐ **Automatic vulnerability scanning**
  Every code library checked against known security issues.
- ☐ **Clean malware scans**
  Each installer scanned with Microsoft Defender and VirusTotal; reports included.
- ☐ **NIST self-assessment**
  Controls mapped to the NIST Cybersecurity Framework (self-assessed).
- ☐ **Cyber liability insurance**
  Certificate of insurance provided.
- ☐ **Microsoft Publisher Verification**
  Microsoft verifies the publisher; blue badge on the approval screen.
- ☐ **Slimmed pilot build**
  Developer and admin tools removed; strict content security settings on.
- ☐ **Full list of components**
  A published list of every library inside the app.
- ☐ **Written policies**
  Privacy policy, data deletion, and incident response.
- ☐ **Your questionnaire answered**
  Your firm's vendor security questions, answered in full.

PLANNED

- ⬚ **Independent penetration test**
  An outside security firm tests the app; report shared with your IT.
- ⬚ **Microsoft 365 Certification**
  Full independent audit under Microsoft's program, as the product grows.
- ⬚ **Microsoft 365 Publisher Attestation**
  Security answers published by Microsoft (eligibility being confirmed).

Checks your IT can run on a test PC

Block the Agendum server in the firewall. Mail reading and the task list keep working; only update checks stop.

Open the app in Microsoft Entra. Its permissions and every sign-in are listed there.

Watch network traffic. Connections go only to Microsoft sign-in, Microsoft mail, and the update server.

Open the saved database file. Email content inside is encrypted and unreadable.

Permissions requested from Microsoft: Mail.Read (read-only), Calendars.ReadWrite (used only when a person clicks "Add to calendar"), User.Read, openid, email, offline_access. A full security pack with the questionnaire answers and policies goes to your IT before approval.