

AGENCY OWNER DISCUSSION GUIDE

Takeaways and key questions to guide internal conversations with your leadership team, staff, and IT partner.

How to use this guide: Bring this to your next leadership or staff meeting. Work through each section, check the box if you can answer confidently, and note who owns any follow-up. Any question you can't answer today is your next step.

KEY TAKEAWAYS FROM TODAY'S SESSION

- ▶ **Own the risk.** Cybersecurity is a business risk, not just an IT issue. Owners make the key decisions during an incident.
- ▶ **Keep the plan real.** Your WISP should match how your agency actually works today, not how it worked when it was written.
- ▶ **Identity is the front door.** Strong MFA, sign-in rules, and limited admin access stop most account takeovers.
- ▶ **Test the restore.** A backup only counts if you've restored from it and know how long it takes.
- ▶ **AI readiness first.** Staff are already using AI. Rules and visibility come before licensing.
- ▶ **Verify every money request.** Wire, ACH, and banking changes are the #1 target. Always call back on a known number.

DISCUSSION QUESTIONS

1. Governance & Your WISP

- ☐ When was our Written Information Security Program (WISP) last reviewed, and who owns it?
- ☐ Does it reflect our current carriers, systems, remote work, and vendors?
- ☐ Do new hires and existing staff receive security training at least once a year?

2. Identity & Access

- ☐ Is MFA required for email, our agency management system, carrier portals, and banking?
- ☐ Who has admin rights, and do they use a separate admin account for admin tasks?
- ☐ How quickly is access removed when an employee or producer leaves the agency?

3. Email, Payments & Fraud

- ☐ What is our written process for verifying wire, ACH, or premium payment changes?
- ☐ Do staff know how to report a suspicious email, and do they feel comfortable doing it?

4. Backup & Recovery

- ☐ When did we last complete a real restore, how long did it take, and was anything missing?
- ☐ Are Microsoft 365 email, OneDrive, and SharePoint backed up separately from Microsoft's defaults?

5. Incident Response

- ☐ If shared files were locked Monday morning, who is the first call, and do we have their number offline?
- ☐ Do we know who contacts our cyber insurance carrier, clients, and legal counsel, and when?

6. AI Readiness

- ☐ **Data:** Do we know which AI tools staff are already using, and what client information goes into them?
- ☐ **Access:** Are file and folder permissions clean enough that an AI assistant won't surface something it shouldn't?
- ☐ **Governance:** Do we have a short, written AI acceptable use policy?
- ☐ **Vendors:** Which third-party tools and vendors can access our company or client data?

SIMPLE RESTORE TEST ANY OWNER CAN ASK FOR

1. Pick one real file or mailbox from last week and ask IT to restore it.
2. Time how long it takes from request to having the file back.
3. Confirm the restored data is complete and current.
4. Write down the result and repeat the test every quarter.

OUR AGENCY'S NEXT STEPS

Priority	Action Item	Owner	Target Date
1			
2			
3			

MEETING NOTES