AI Deployment Readiness Checklist

Work through this before enabling any AI tool in your family office environment.

Governance and Controls — Do This Before Anything Else

- [ ] Write your AI governance policy before any tool goes live.
- [ ] Add an AI use policy to your employee handbook. Specify which tools are approved and explicitly prohibit personal AI accounts for work of any kind.
- [ ] Establish that any work product created using AI tools belongs to the organization, not the individual.
- [ ] Update your vendor agreements to address AI usage and data handling obligations.
- [ ] Note applicable regulatory requirements — HIPAA, FINRA, SEC, state AI laws — and ensure your policy reflects them.
- [ ] Communicate the policy to all staff before deployment, not after.

Before You Turn It On

- [ ] Catalog your data: what it is, where it lives, who can access it.
- [ ] Archive or remove sensitive data that has no reason to be AI-accessible.
- [ ] Apply sensitivity labels to data by category.
- [ ] Decide which AI tools are approved and which are off-limits until fully evaluated.
- [ ] Use enterprise-licensed accounts only. Free-tier tools can use your data to train their models.

Configuration

- [ ] Start with a small pilot group of 3–5 users before any wider rollout.
- [ ] Run the pilot for at least 30 days. Have the group actively try to find gaps — what data can be seen that shouldn't be accessed, what the tool can reach that it shouldn't.
- [ ] Start in read-only or sandbox mode. Expand access deliberately, not all at once.
- [ ] Restrict connectors. The AI should not have default access to personal or family archives.
- [ ] Turn off model learning on your data wherever the setting exists.
- [ ] Set retention and deletion policies for prompts and AI-generated outputs.

201 Centennial Street, Ste 112 • Glenwood Springs, CO 81601 • 855.808.6920 • info@decyphertech.com • www.decyphertech.com

Access Controls

- [ ] Limit access by role. Not everyone needs to see everything.
- [ ] Encrypt data at rest and in transit.
- [ ] Test it: can someone reach HR or financial data through the AI? They should not be able to.

Ongoing

- [ ] Train staff on approved tools, prohibited inputs, and how to recognize AI-generated phishing and impersonation attempts.
- [ ] Require human review for any AI-generated content touching legal, financial, or reputational decisions.
- [ ] Extend your AI policy to vendors and partners, not just your internal team.
- [ ] Maintain an AI-specific incident response plan — know what you will do if a breach or data exposure involves an AI tool.
- [ ] Build audit trails for any AI action involving payments, personal data, or file transfers.