🛟 Organization AI Security Preparedness Short List

Sandy Dunn

Who Should Use This Checklist?

- ★ CISOs, Security Architects, Developers
- ★ Chief Data Officers, Privacy Officers
- ★ Risk and compliance teams
- ★ Procurement teams

Important AI Preparedness Tasks

- ☐ **Confirm legal and regulatory compliance** to ensure all obligations are current and aligned with evolving AI and data privacy standards.
- ☐ **Review and strengthen fraud detection processes**, especially for invoicing, financial transactions, and hiring workflows, to mitigate threats from deepfakes or AI generated material.
- ☐ **Update the Incident Response Plan** to include AI related incidents, including strategies for detecting and responding to disinformation.
- ☐ **Audit third-party partners** to identify any changes in functionality, AI feature integration, or updates to data usage terms that may impact your data use standard.
- ☐ **Revise the third-party risk questionnaire** to include AI specific questions, especially around model usage, training data, and generative capabilities.
- ☐ **Establish or update the organization's AI Policy**, or revise the Acceptable Use Policy to address the use of AI tools to restrict the use of company data in external or unauthorized AI systems.
- ☐ **Conduct employee training on AI threats and responsible use**, including how to recognize deepfakes, AI generated phishing, and misuse of generative tools.

QR Link for additional Checklists

- ★ 🍩 AI System Card Review Checklist
- ★ 🚨 2025 IR Update Checklist AI Incident Response
- ★ 🚨 2025 SIEM Run book for GenAI Incident Investigation
- ★ 🧮 AI Updates for Organization's Enterprise Risk Register