AI Productivity Safety Checklist

Use this checklist to evaluate your organisation's readiness for safe and responsible AI productivity adoption.

Check each item currently in place.

AI Productivity Safety Assessment

☐ 1. We have identified which AI tools are officially approved for employee use.

☐ 2. Employees understand what information should never be entered into AI systems.

☐ 3. We prohibit employees from entering passwords or credentials into AI tools.

☐ 4. Customer data handling rules apply to AI usage.

☐ 5. We have an internal AI usage policy.

☐ 6. Employees understand the risks of AI-generated phishing and impersonation attacks.

☐ 7. We train employees to verify suspicious requests and unusual communication.

☐ 8. AI-generated content is reviewed before external distribution.

☐ 9. We educate employees about AI hallucinations and inaccurate outputs.

☐ 10. Employees know how to report suspicious AI-related activity.

☐ 11. We review AI vendors before approving business use.

☐ 12. We understand how approved AI platforms process and store data.

☐ 13. We restrict confidential information from being uploaded into unapproved AI systems.

☐ 14. Employees understand intellectual property risks related to AI usage.

☐ 15. Remote and hybrid workers receive AI security awareness training.

☐ 16. Managers reinforce safe AI usage expectations consistently.

☐ 17. We maintain multi-factor authentication for business systems and AI-related accounts.

☐ 18. We educate employees about fake AI tools and malicious browser extensions.

☐ 19. AI usage expectations are communicated clearly in practical language.

☐ 20. We regularly review and update AI governance procedures.

☐ 21. Employees understand when human review is required for AI-generated work.

☐ 22. Sensitive HR, legal, financial, and customer data is restricted appropriately.

☐ 23. Leadership understands both the productivity and cybersecurity implications of AI adoption.

☐ 24. Verification procedures exist for payments, approvals, and sensitive requests.

☐ 25. We treat AI governance as an ongoing operational responsibility rather than a temporary trend.

Scoring Guide

Strong Maturity

20–25 checked items

Your organisation demonstrates strong readiness for safe AI productivity adoption. You likely have practical governance, employee awareness, leadership engagement, and cybersecurity discipline supporting AI usage.

Continue focusing on:

- policy refinement,
- awareness updates,
- vendor oversight,
- and operational consistency.

Moderate Exposure

12–19 checked items

Your organisation has meaningful awareness of AI-related risk, but important gaps still exist.

You may need stronger:

- employee training,
- verification procedures,
- policy consistency,
- or leadership involvement.

Improving operational clarity and governance should become a near-term priority.

High Vulnerability

0–11 checked items

Your organisation may face significant exposure from unsafe AI usage practices.

Employees may be using AI tools without:

- sufficient oversight,
- practical guidance,
- or consistent security awareness.

Immediate improvement is recommended in:

- governance,
- employee education,
- sensitive data handling,

and AI-related cybersecurity awareness.