AI USE & BOUNDARIES CHECKLIST

ORCHESTRATO

1. Define Purpose & Scope

- What business outcomes are you aiming for with AI?
- Which teams and processes will use AI tools?

2. Identify Sensitive Data

- List data categories that must never leave your environment (e.g., Personal Identifiable Information, financials, IP).
- Confirm masking or anonymisation for any data used in AI workflows.

3. Approved Tools & Access

- Maintain a list of authorised AI platforms and integrations.
- Enforce role-based access controls and MFA for all AI-related systems.

4. Public vs Private LLM Usage

- Prohibit uploading sensitive business/customer data to public LLMs.
- Route all AI interactions through secure gateways or enterprise tenants.

5. Data Governance Alignment

- Ensure AI use complies with existing InfoSec and Data Protection policies.
- Update DLP rules and monitoring for AI-specific risks.

6. Logging & Audit

- Enable logging for prompts, outputs, and data transfers.
- Review audit trails regularly for anomalies or policy breaches.

7. Shadow AI Prevention

- Communicate clear guidance on approved tools.
- Provide an easy process for requesting new AI solutions.

AI USE & BOUNDARIES CHECKLIST

ORCHESTRATO

8. Training & Awareness

- Deliver short, role-based training on safe AI use and data boundaries.
- Include examples of acceptable vs prohibited practices.

9. Incident Response

- Add AI-specific scenarios to security playbooks (e.g., prompt leakage, misuse).
- Define escalation paths for suspected breaches.

10. Continuous Review

- Revisit this checklist quarterly as AI use cases evolve.
- Align updates with regulatory changes and business priorities.

Disclaimer:
This report is provided for informational purposes only. While Orchestrato Ltd. has made every effort to ensure the accuracy and reliability of the information contained herein, no representation or warranty, express or implied, is made as to its completeness, accuracy, or fitness for any particular purpose. The data and analysis presented are based on sources believed to be reliable, but may be subject to change without notice. Orchestrato Ltd. accepts no liability for any loss or damage arising from reliance on this report or its contents. Recipients should seek their own independent advice before making any decisions based on the information provided.