Below is a general AI Policy Framework designed for companies with between 50 and 500 employees. This framework is tailored for a BoardPro webinar on practical use cases for AI in governance and is crafted to guide organisations in responsibly adopting and overseeing AI technologies.

**General AI Policy Framework for Mid-Sized Companies**

**1. Introduction**

As organisations embrace artificial intelligence, it is essential to establish a robust framework that balances innovation with responsible governance. For companies with 50 to 500 employees, this framework serves as a practical guide to:

* **Protect critical data and intellectual property**
* **Manage regulatory and operational risks**
* **Foster a culture of transparency and accountability**
* **Empower board members and executives with clear oversight**

Think of this framework as building a secure and agile "AI fortress"—one that allows innovation while safeguarding your organisation from potential vulnerabilities.

**2. Governance and Oversight**

**Objective:**
Ensure that AI initiatives align with the company’s strategic goals and regulatory obligations while establishing clear accountability at all levels.

**Key Elements:**

* **Board and Executive Responsibility:**
	+ The board should oversee AI strategy, risk management, and compliance.
	+ Establish an AI Governance Committee, including key executives, to review AI initiatives regularly.
	+ Define clear roles for oversight, including appointing a Chief AI Officer or a similar role, even if on an interim basis.
* **Policy Alignment:**
	+ Ensure that the AI policy integrates with the organisation’s broader risk management and compliance frameworks.
	+ Regularly update the AI policy to reflect evolving regulatory requirements and technological advancements.
* **Strategic Review:**
	+ Hold periodic strategic reviews of AI projects to ensure alignment with business objectives.
	+ Use these reviews to decide whether to expand, adjust, or phase out certain AI initiatives.

**3. Risk Identification and Management**

**Objective:**
Identify and mitigate risks associated with AI adoption, ensuring that potential vulnerabilities are proactively managed.

**Key Elements:**

* **Risk Categories:**
	+ **Data Protection:** Ensure AI systems comply with data privacy regulations (e.g., GDPR) by implementing robust data management practices.
	+ **Intellectual Property (IP):** Protect proprietary algorithms and innovations through clear IP policies.
	+ **Cybersecurity:** Adopt strong security measures to defend against hacking and unauthorised access, including regular vulnerability assessments.
	+ **Ethical Considerations:** Address biases and fairness in AI by establishing guidelines for ethical AI use.
	+ **Operational Risks:** Consider the impact on business continuity and ensure that AI systems are resilient and well-integrated with existing operations.
* **Risk Assessment:**
	+ Conduct a comprehensive risk assessment for all AI projects before deployment.
	+ Develop a risk register that includes identified risks, their potential impact, and mitigation strategies.
* **Oversight and Accountability:**
	+ Designate specific teams or individuals responsible for monitoring AI risks.
	+ Implement clear escalation procedures if risks materialise, ensuring that board members are promptly informed.

**4. Do’s and Don’ts Policy**

**Objective:**
Establish clear, actionable guidelines that direct the responsible use of AI while preventing potential missteps.

**Key Elements:**

* **General Principles:**
	+ **Do:**
		- Ensure all AI initiatives align with company values and regulatory requirements.
		- Obtain necessary approvals and conduct thorough risk assessments before launching AI projects.
		- Maintain transparency in AI decision-making processes and ensure accountability.
		- Regularly update internal controls to include AI-specific risks.
	+ **Don’t:**
		- Deploy AI systems without proper risk assessment and management.
		- Rely solely on AI for critical decisions without human oversight.
		- Overlook the importance of secure data handling and vendor compliance.
		- Ignore emerging risks or fail to update policies as new challenges arise.
* **Vendor Management:**
	+ **Do:**
		- Ensure external AI vendors adhere to your organisation’s standards, with clear contractual terms that include compliance, data protection, and security obligations.
	+ **Don’t:**
		- Engage vendors without verifying their compliance with relevant standards and regulations.
* **Data Handling and Confidentiality:**
	+ **Do:**
		- Secure all data inputs and outputs from AI systems, using encryption and regular audits.
	+ **Don’t:**
		- Compromise on data security for the sake of expediency.

**5. Role-Based Guidance**

**Objective:**
Provide tailored instructions for various departments to ensure everyone in the organisation knows their role in upholding the AI policy.

**Key Elements:**

* **Marketing:**
	+ **Responsibilities:**
		- Use AI for personalised customer communications while ensuring data protection and compliance.
	+ **Guidelines:**
		- **Do:** Verify data sources and validate AI outputs.
		- **Don’t:** Use AI-driven insights without proper oversight.
* **Human Resources (HR):**
	+ **Responsibilities:**
		- Leverage AI in recruitment and employee management without introducing bias.
	+ **Guidelines:**
		- **Do:** Ensure that AI tools support fair and transparent processes.
		- **Don’t:** Rely entirely on AI for recruitment decisions; maintain human oversight.
* **IT/Cybersecurity:**
	+ **Responsibilities:**
		- Oversee the secure implementation and maintenance of AI systems.
	+ **Guidelines:**
		- **Do:** Implement regular security audits and keep systems updated.
		- **Don’t:** Circumvent established security protocols for speed or convenience.
* **Legal/Compliance:**
	+ **Responsibilities:**
		- Ensure all AI implementations comply with relevant regulations and internal policies.
	+ **Guidelines:**
		- **Do:** Review and approve all AI initiatives for compliance.
		- **Don’t:** Allow AI projects to proceed without a full legal and compliance review.

**6. Communication and Training**

**Objective:**
Ensure that the AI policy is clearly communicated across the organisation and that employees are equipped to follow it effectively.

**Key Elements:**

* **Communication Channels:**
	+ Disseminate the AI policy through the company intranet, email updates, and regular town hall meetings.
	+ Use short presentations and infographics to simplify key concepts.
* **Training Programs:**
	+ Organise webinars and interactive training sessions to educate employees on AI risks, best practices, and their specific responsibilities.
	+ Develop simple, accessible training materials like FAQs, quick-reference guides, and video tutorials.
* **Feedback Mechanisms:**
	+ Establish channels for employees to ask questions, report issues, or provide suggestions related to the AI policy.
	+ Regularly review and integrate feedback to improve the policy and training methods.

**7. Ongoing Monitoring, Review, and Incident Response**

**Objective:**
Maintain a dynamic and resilient AI policy through regular monitoring, reviews, and a structured response plan for any incidents.

**Key Elements:**

* **Monitoring and Audits:**
	+ Schedule periodic audits (e.g., quarterly or bi-annually) to assess compliance with the AI policy.
	+ Use monitoring tools to track AI system performance, data handling, and compliance adherence.
* **Incident Response:**
	+ Develop a clear process for handling any breaches, non-compliance issues, or unexpected AI behaviours.
	+ Define escalation procedures and designate responsible teams to manage and resolve incidents.
* **Policy Updates:**
	+ Set an annual review cycle to update the AI policy in line with new technologies, evolving regulations, and lessons learned from past incidents.
	+ Document all changes and communicate updates promptly to ensure ongoing compliance.

**8. Conclusion**

A comprehensive AI policy framework is crucial for mid-sized companies to harness the benefits of AI while managing the inherent risks. By implementing this framework, organisations can:

* Ensure robust governance and clear oversight at all levels.
* Identify and mitigate risks through proactive measures and regular assessments.
* Establish clear guidelines that align with best practices and regulatory requirements.
* Empower departments with tailored guidance to maintain transparency, security, and accountability.
* Foster a culture of continuous improvement through effective communication, training, and regular reviews.

This framework not only serves as a shield protecting your organisation’s interests but also as a catalyst for responsible and innovative use of AI. For board members and executives, it provides a clear structure to oversee AI initiatives, ensuring they contribute positively to the organisation’s long-term success.

This general AI policy framework can be adapted and refined as your company’s AI journey evolves. It is designed to be a living document—one that grows with your organisation, ensuring that innovation is always balanced with the highest standards of governance and risk management.