SALLENBACH

AI & Innovation Consulting

AI Governance Policy for Boards and Portfolio Companies

Clear guardrails for responsible AI use, strategic control and effective board oversight.

Enable	AI is used where it improves research, drafting, structuring, quality assurance, administration and board preparation.
Protect	Mandate files, board papers, personal data, professional secrecy and strategic information remain protected.
Prove	Material AI use is documented by tool, purpose, data zone, responsible person, controls and human review.

Model Policy for the BoardCompliance AG / BoardPlus Context

Showcase context: Dr. Leonz Meyer, BoardCompliance AG / BoardPlus

Homepage Edition | June 2026 | Sallenbach AG | AI & Innovation Consulting | www.sallenbach.org | vero@sallenbach.org

What this policy is for

It is designed as a pragmatic starting point: boards can share it with portfolio or mandate companies, executive management can derive internal rules from it, and teams receive clear guardrails for daily AI use.

Note for Leonz / BoardCompliance: Legal mandate work, board papers and consular communications require heightened care. Public chatbots are not suitable for such data; only explicitly approved and contractually reviewed environments should be used.

Message to employees

Dear colleagues

Artificial intelligence is increasingly part of everyday work: in emails, office tools, research, presentations, meeting notes, data analysis and automated workflows. We want to use these opportunities, but with clear guardrails.

This AI Governance Policy explains which data may be entered into which tools, when approval is required, how AI outputs must be reviewed and how uncertainties or incidents should be reported.

Please use AI pragmatically, but consciously: do not enter confidential, personal, mandate-related, market-sensitive or protected information into non-approved public AI tools; review outputs critically; keep sources traceable; raise uncertainties early.

This policy is a starting point. Questions, tool suggestions or uncertainties can be addressed to the person responsible for AI, data protection, legal or compliance.

Kind regards
[Board of Directors / Executive Management]

Data Zone Compass

The zones translate abstract confidentiality and data protection duties into a simple working rule: identify the data zone first, then choose the tool.

Zone	Data Examples	Rule
Green: Public	Public information, website copy, already published content, general ideas and non-sensitive prompts.	Public AI tools may be used, provided the prompt does not reveal confidential or hidden sensitive information.
Yellow: Internal	Internal non-confidential drafts, anonymised examples, general process ideas and working notes.	Use approved business or enterprise tools only; avoid unnecessary personal, client or mandate data.
Orange: Sensitive	Personal data, HR matters, client lists, internal financials and unpublished management information.	Use only approved tools with clarified hosting, access control, deletion, contractual basis and role permissions.
Red: Confidential / Professional Secrecy	Mandate files, legal questions, board papers, M&A, crisis matters, consular and client communications.	Do not use public AI tools. Use only explicitly approved secure legal or enterprise environments.
Black: Highest Protection	Inside information, disputes, investigations, highly sensitive strategy or transaction data.	AI use only after case-by-case approval by legal, compliance or the board and with a documented protection concept.

1. Purpose and Scope

This model AI Governance Policy governs the responsible use of artificial intelligence in companies overseen by a board of directors, supervisory board or comparable governance body. It applies to board members, executive management, employees, external advisers, freelancers and any other persons working with AI systems on behalf of the company.

The purpose is to enable AI use without compromising confidentiality, data protection, trade secrets, professional secrecy, intellectual property rights, reputation, decision quality or regulatory duties.

For the BoardCompliance / BoardPlus context, an additional practical anchor applies: mandate files, board papers, legal assessments, consular communications and client questions are generally highly sensitive and must not be entered into public AI tools.

2. Board Principles

Human accountability remains non-delegable: AI supports analysis, drafting, structuring and quality assurance. Decisions of the board, committees and executive management are not delegated to AI.

Confidentiality first: confidential board papers, strategy, finance, HR, M&A, legal and client data may only be processed in approved and contractually reviewed environments.

Value before hype: AI is used where it enables better preparation, faster orientation, higher quality or stronger controls.

Transparency and traceability: material AI use is documented by tool, purpose, data class, responsible person, approval and review steps.

Security and privacy by design: before use, new AI applications are reviewed for data flows, hosting, training, human review, access, logging, deletion and exit options.

3. Roles and Responsibilities

Board of Directors / Supervisory Board: approves principles, risk appetite, material AI initiatives and annual reporting. It requires an AI register and reviews critical use cases.

Board committees: review AI risks relevant to their mandate. Audit, risk and compliance committees focus on controls, privacy, information security and reporting quality.

Executive management: implements this policy, appoints responsible persons, maintains the tool and use-case register, and ensures training and controls.

AI responsible person: reviews tools, coordinates approvals, documents risks and manages incident response.

Users and external contributors: comply with data zones and approvals, critically review outputs and immediately report misconduct, data leakage or critical outputs.

4. Permitted Board Use Cases

Board briefings: summaries of regulatory, technological or market developments. Sources must be checked; confidential inputs may not be entered into non-approved tools.

Meeting preparation: agenda drafts, question lists, risk matrices and decision options. Final papers require approval by the responsible person.

Policy and playbook drafting: first drafts for AI policies, data protection, information security, delegation rules or crisis playbooks. Legal review remains mandatory.

Risk registers and control questions: identification of weaknesses, measures and monitoring questions. Risks should be prioritised and documented in a board-traceable manner.

Training, AI avatars and simulation: board scenarios on cyber, crisis, media, liability, the EU AI Act or data protection. AI avatars must be identifiable as such; image, voice and script rights must be clarified.

5. Prohibited or Approval-Only Use

No confidential, personal, mandate-related, market-sensitive or professionally secret information may be entered into non-approved public AI tools.

No automated decisions on employment, remuneration, credit, insurance, benefits, termination or access to services without separate legal review.

No covert transcription, recording or analysis of board meetings without prior information, legal basis, tool approval and clear retention or deletion rules.

No publication of AI-generated statements, figures, legal assertions, financial information or avatar videos without independent review and approval.

No autonomous AI-agent communication with clients, authorities, investors or media without defined approval thresholds and human final control.

6. Tool Approval and AI Register

Before productive use, each AI tool requires approval. The board requires at least a lean AI register, reviewed annually or whenever material changes occur.

The register documents purpose, use case, tool, data zone, responsible person, data flows, hosting, training or human review by the provider, access, deletion, controls and status.

Particular attention must be paid to zero data retention, no human review, subprocessors, third-country transfers, CLOUD Act exposure, role rights, logging, contractual basis and exit options.

7. Quality Assurance and Human-in-the-loop

AI outputs are working drafts. The person using AI remains responsible for accuracy, completeness, timeliness, appropriateness, tone and legal robustness.

Facts, figures, quotations, legal assertions and sources must be independently checked. Legal, financial, regulatory or reputational matters require qualified second review.

Board papers must not contain unchecked AI claims. Material assumptions, uncertainties and data gaps are made transparent.

8. Board Meetings, Minutes and Confidential Rooms

Board meetings require heightened safeguards. AI-supported transcription, summarisation, translation or analysis is permitted only where purpose, participant information, tool approval, data storage, deletion and access are clearly regulated.

Board rule: no AI recording of meetings without prior information and defined retention or deletion logic. Crisis, M&A, personnel, legal and inside-information topics are generally Red or Black zone matters.

9. Agentic Workflows and Automation

AI agents that independently research, draft emails, query data, book appointments, modify documents or trigger external systems require separate approval.

Agents receive only the minimum rights required. External communications, payments, contract changes and data exports require human confirmation.

Actions, inputs, outputs and approvals must be traceable. Responsible persons must be able to deactivate the agent at any time. New agents are first tested with dummy data, limited scope and clear success criteria.

10. Incident Response

Every person must immediately report if confidential data has been entered into the wrong tool, an AI system has obtained unauthorised access, a critical wrong output has been used, or there are indications of data leakage, manipulation, bias or security breach.

Immediate measures: stop the use, publication or agent action; document time, tool, prompt, output, affected data and involved persons; escalate to the AI responsible person, legal, data protection, IT security and, where appropriate, the board chair.

Board Quick Check

Twelve questions for the next board or executive management meeting.

#	Control Question	Status
1	Has an AI Governance Policy been approved and communicated to all relevant persons?	□ Yes □ Partly □ No
2	Are data zones defined, especially for board, mandate, HR, financial and client data?	□ Yes □ Partly □ No
3	Is there a list of approved AI tools and clear prohibitions for public tools?	□ Yes □ Partly □ No
4	Have training, human review, data storage, deletion and subprocessors been reviewed for each tool?	□ Yes □ Partly □ No
5	Is material AI use documented in an AI register?	□ Yes □ Partly □ No
6	Is human review mandatory before AI outputs are used externally or for decisions?	□ Yes □ Partly □ No
7	Are there rules for AI in board meetings, transcription, minutes and translation?	□ Yes □ Partly □ No
8	Are AI avatars, synthetic voices and AI-generated communications labelled and approved?	□ Yes □ Partly □ No
9	Are agentic workflows governed by approval thresholds, logging and a kill switch?	□ Yes □ Partly □ No
10	Is there an incident process for wrong outputs, data leakage, bias or wrong tool use?	□ Yes □ Partly □ No
11	Are employees, freelancers and external advisers trained and contractually bound?	□ Yes □ Partly □ No
12	Does the board receive at least an annual AI status report covering opportunities, risks and actions?	□ Yes □ Partly □ No

Appendix A: Lean AI Register

Use Case	Tool	Owner	Data Zone	Benefit	Risk	Control	Status
Board Briefing	[Tool]	[Name]	Yellow/Red	faster preparation	wrong sources	source check	pilot
Minutes Draft	[Tool]	[Name]	Red	time saving	confidentiality	approval + deletion	to review
AI Avatar Training	[Tool]	[Name]	Yellow	training scale	deception/rights	labelling	pilot

Appendix B: 30-60-90 Day Plan

Timeline	Focus	Outcome
30 days	**AI status view**	Map tools, shadow AI, data zones, quick wins and immediate rules.
60 days	**Approval & training**	Set up tool review, responsibilities, pilot use cases, training and the AI register.
90 days	**Embed governance**	Institutionalise reporting, review rhythm, incident process and board control questions.

Appendix C: Tool Approval

Review points	Data storage, training, human review, subprocessors, contracts, role rights, logging, deletion, exit options and support.
Approval threshold	The more confidential the data and the more external the effect, the higher the control: from team approval to board or legal decision.

Legal Anchors and Sources

This model policy does not replace company-, sector- or case-specific legal review. It is based on publicly available guidance and legal anchors.

Swiss Bar Association: Guidelines on the use of artificial intelligence: https://www.sav-fsa.ch/documents/672183/2025869/SAV_KI%2BGuidelines%2B2024.pdf/68d5eab4-c2ad-50bd-506f-7ba6af15a839?t=1726488889628
FDPIC: Artificial intelligence and data protection: https://www.edoeb.admin.ch/en/ai-and-data-protection
Fedlex: Swiss Federal Act on Data Protection: https://www.fedlex.admin.ch/eli/cc/2022/491/en
Fedlex: Art. 321 Swiss Criminal Code, professional secrecy: https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en#art_321
EUR-Lex: Regulation (EU) 2024/1689, Artificial Intelligence Act: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

---

Sallenbach AG | AI & Innovation Consulting | www.sallenbach.org | vero@sallenbach.org