

Company Generative AI Usage Policy - Template (2026 Edition)

Replace every [highlighted placeholder] with your organization's details before publishing.

Introduction

This policy outlines the acceptable use of Generative AI (GenAI) technologies within our company. Our goal is to harness GenAI's capabilities to enhance business operations while ensuring ethical, secure, and compliant usage.

Scope

This policy applies to all employees, contractors, and partners who utilize GenAI tools in their work-related activities.

Approved Tools & Accounts

- **Approved Tools List:** Use only GenAI tools approved by IT and Security. The approved list is maintained at [location] and reviewed every quarter.
- **Company Accounts Only:** Use work data only in company-provided accounts (business or enterprise plans, where our data is not used to train models). Never paste work data into a personal account, free or paid.
- **New Tools:** Want to use a tool that is not on the list? Submit a request to [owner]. Browser extensions, AI note-takers and AI features inside existing software (CRM, email, design tools) count as new tools too.

Acceptable Use

To use GenAI effectively and responsibly:

- **Data Protection:** Do not input personal information, including full names, addresses, phone numbers, social security numbers, or any other personally identifiable information.
- **Data Traffic Light:** Green (public information): any approved tool. Yellow (internal information): company accounts only. Red (customer personal data, financials, credentials, unreleased plans): only in tools explicitly approved for that data type, or not at all.
- **Anonymization:** When discussing personal scenarios or examples, use fictional or generic names.
- **Fact-Checking:** AI-generated responses may contain factual errors, biases, or inappropriate content. Always verify accuracy before using or distributing AI-generated outputs.
- **Professionalism:** Ensure AI-generated content remains professional, respectful, and free from offensive, discriminatory, or inappropriate language.
- **Security Measures:** Protect access credentials and prevent unauthorized access to GenAI systems.

- **Compliance:** Follow all applicable laws, regulations, and company policies when using GenAI tools.

Prohibited Use

The following actions are strictly prohibited when using GenAI:

- **Confidential Information:** Do not input, share, or expose sensitive data, including:
 - Passwords, credit card numbers, health records, or any other confidential information.
 - Company intellectual property (IP) or trade secrets unless explicitly authorized.
 - Any proprietary or business-sensitive data in external AI tools (such as ChatGPT) unless privacy settings (e.g., history/cache disabling) are properly configured.
 - Privacy toggles in a personal account are not enough for business data. Business-sensitive data goes only into approved company accounts.
- **Inappropriate Content:** Do not generate, distribute, or use AI to create:
 - Illegal, discriminatory, defamatory, or otherwise inappropriate content.
 - Harassing, bullying, or intimidating messages.
 - Fake images, audio or video of real people (deepfakes), including colleagues, customers and public figures.
- **Security Risks:** Avoid activities that could compromise the security or integrity of the company's data and systems.
- **Misinformation:** Do not knowingly distribute false or misleading information generated by AI.

AI Agents & Automations

AI tools no longer just answer. They send emails, edit files, update systems and run tasks on their own. These rules apply to any agent, automation or connector:

- **A Human Approves:** An agent may draft and prepare. A person approves any action that is external or hard to undo: sending messages, publishing, payments, deleting data, changing permissions.
- **Minimum Access:** Connect an agent only to the systems and folders the task needs. Connecting an agent to company email, file storage, CRM or code requires IT approval.
- **Untrusted Inputs:** Websites, emails and documents an agent reads may contain hidden instructions (prompt injection). Agents must not act on instructions found inside content they process.
- **Named Owner:** Every agent and automation has a named owner who is responsible for its output and its access.

Responsibilities

- **Employees:** Ensure compliance with this policy in all AI-related activities.

- **Managers:** Educate teams and enforce policy adherence.
- **Legal & Compliance Team:** Oversee regulatory compliance and address concerns related to AI usage.
- **AI Ethics Team:** Monitor ethical considerations, bias, and responsible AI use.
- **IT & Security:** Maintain the approved tools list, approve agent connections, and review access regularly.

Training & AI Literacy

- **Basic Training:** Every employee completes basic GenAI training before receiving access to approved tools, with a short refresher every year.
- **EU Note:** Organizations operating in the EU must take measures to support AI literacy among staff who use AI (EU AI Act, Article 4, as amended by the Digital Omnibus, Regulation (EU) 2026/1744).

Privacy and Data Protection

- **Personal Data Handling:** Comply with privacy laws when processing personal data in GenAI tools. Obtain necessary consent where applicable.
- **Data Anonymization:** De-identify personal data before inputting it into AI systems to mitigate privacy risks.
- **Audit & Logging:** When feasible, maintain logs of AI interactions for compliance reviews without compromising security.
- **Meetings & Recordings:** Tell participants before an AI tool records or transcribes a meeting. If anyone objects, don't record.
- **Incident Reporting:** Entered sensitive data into an unapproved tool by mistake? Report it to **[owner]** within 24 hours. Fast reporting is never punished.

Ethical Considerations

- **Bias and Discrimination:** Regularly review AI-generated decisions for potential biases. Implement corrective measures as needed.
- **Intellectual Property:** Do not use copyrighted materials or third-party proprietary content without proper authorization.
- **Accountability:** Employees are responsible for the ethical use of AI and should report any concerns about misuse.

Review and Compliance

- **Policy Updates:** This policy will be reviewed annually to ensure ongoing relevance and effectiveness.
- **Interim Updates:** The policy is also reviewed whenever the company adopts a major new AI tool or capability (for example, AI agents).
- **Regulatory Map:** Check which laws apply to your organization, for example Israel's Privacy Protection Law (Amendment 13, in force since August 2025), GDPR and the EU AI Act.
- **Violations:** Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

Transparency

- **Disclosure:** Employees must clearly disclose when GenAI has been used in the creation of external-facing content, products, or services.

Conclusion

Adhering to this policy ensures responsible, ethical, and secure use of GenAI technologies within our company. It aligns with our values, regulatory obligations, and commitment to innovation. For further guidance or questions, please contact the **Legal & Compliance Team**.

Template made by:

[Eyal Marcus](#), not a lawyer, not responsible for your usage of the template (that needs editing and customization to your org)

I encourage you to subscribe to [my weekly newsletter](#) - it's packed with content that will help you stay ahead of the curve.

And don't forget to check out my podcast, you won't believe what it's about (hint: it's about Gen AI).