AI ACCEPTABLE USE POLICY

PREPARED FOR

Company Name

Template Prepared By:

Techtron Computers (Pty) Ltd

CONTENTS

techtron

ARTIFICIAL INTELLIGENCE (AI) ACCEPTABLE USE POLICY

Version: 1.0

Effective Date: [INSERT DATE]

Document Owner: [INSERT NAME]

Company Name: [INSERT COMPANY NAME]

1. OUR APPROACH TO AI

Artificial Intelligence offers incredible opportunities for leverage, creativity, and efficiency. We want you to use these tools to do the best work of your career. However, these tools also introduce new risks—from data leakage to copyright issues—that can threaten our business, our clients, and our reputation.

We have created this policy to ensure we are all using AI safely and responsibly.

Our goal is to protect the company over the long term so that we can continue to innovate without putting our hard work at risk. Please read this carefully; it is the roadmap for how we work with AI.

2. PERSONAL RESPONSIBILITY

You are responsible for the accuracy, legality, and privacy of any work you submit.

AI is a tool, not an employee. Using AI doesn't excuse errors, bias, or copyright infringement. You must verify all AI-generated outputs. If you use AI to generate a report, piece of code, or email, you own the final result.

Think of AI as a "Junior Assistant." It is fast, eager, and helpful, but it doesn't know our business context, our clients, or our ethical standards like you do. Always review its work with a critical eye. Your professional judgment is the final filter before anything leaves your desk.

3. KEY DEFINITIONS

To make this policy easy to read, we want to make sure everyone is on the same page regarding the technical terms used throughout the document. AI has its own language, and understanding these few key definitions will help you understand the "Why" behind our rules.

- **Generative AI:** Artificial intelligence capable of creating new content (text, images, code) in response to prompts (e.g., ChatGPT, Midjourney).

- **Hallucination:** A phenomenon where an AI confidently generates false, misleading, or nonsensical information

- **Training Data:** Information fed into an AI model to teach it. If company data is used as "Training Data" by a public AI tool, that data may become part of the public model and be leaked to others.

- **Shadow IT:** The use of unauthorized or unvetted software by employees without IT department approval.

- **Jailbreaking / Prompt Injection:** The act of using specific inputs to trick the AI into getting around its safety filters or security rules.

- **PII (Personally Identifiable Information):** Any data that could potentially identify a specific individual (e.g., names, SSNs, addresses, phone numbers).

- **Anonymization:** The process of removing or masking sensitive details (like names or prices) from a document before sharing it with an AI tool.

- **Deepfake:** Synthetic media (video, audio, image) created by AI to convincingly look or sound like a real person, often used for impersonation or fraud.

- **API (Application Programming Interface):** A software bridge that allows two applications to talk to each other. Automation tools (like Zapier) use APIs to send data between systems.

- **Human Oversight:** A process requiring human intervention or approval before an AI decision is finalized.

- **BYOD (Bring Your Own Device):** The practice of employees using their own personal devices (smartphones, tablets) for work purposes.

4. SCOPE OF POLICY

This policy applies to all forms of AI usage, including but not limited to:

- **Web-based Tools:** (e.g., ChatGPT, Claude, Gemini).
- **Browser Extensions:** (e.g., Grammar checkers, page summarizers).
- **Operating System Features:** AI features embedded in Windows, macOS, iOS, or Android (e.g., Copilot in Windows, Apple Intelligence).
- **Meeting Recorders:** Automated transcription tools.

Note: AI Features & Tools pre-installed on company devices are also covered by this policy.

5. AUTHORIZED AND PROHIBITED SOFTWARE

To ensure data security, we restrict which AI tools may be used for business purposes.

Using unvetted tools exposes the company to "Shadow IT" risks, where data is slowly siphoned off to train public models or stored on insecure servers outside of our control.

You may only use AI Tools and Vendors that have been formally approved and set up by the IT Department.

Expenses for unapproved AI tool subscriptions are prohibited and will not be reimbursed.

Please refer to [APPENDIX A] for the current list of Authorized AI Software.

⚠️ Any AI tool, browser extension, or plugin that is **NOT** listed in **[APPENDIX A]** is strictly prohibited.

We do not maintain a list of "Banned Apps" because new tools appear every day. Unless a tool has been vetted and added to the Authorized List, you may not use it for company business.

6. REQUESTING NEW TOOLS

We encourage innovation. If you would like to request an AI Tool or Vendor to be added to our Authorized Software list, **please contact** IT Support or your manager.

They will work with your IT Support Team to perform an AI Vendor Review process.

This "Due Diligence" review covers Privacy, Security, and Data Governance to make sure the tool is safe for our environment.

7. DATA CLASSIFICATION PROTOCOL

You must classify data **before** entering it into any AI tool. Use the table below to determine what is safe.

CLASSIFICATION	AI RATING	DESCRIPTION	REQUIREMENTS	EXAMPLES
PUBLIC DATA	🟢 **SAFE**	Information already available in the public domain.	**No restrictions.**	Marketing copy General industry research Brainstorming
INTERNAL DATA	🟡 **CAUTION**	Internal business documents that are not confidential.	**Anonymization Required.**	Internal Memos Process Documentation Draft Emails
RESTRICTED DATA	🔴 **PROHIBITED**	Any data that would cause harm if leaked.	**NEVER input into AI.**	**PII:** Client Names, SSNs, Home Addresses **Financials:** Bank Accts, Credit Cards **Credentials:** Passwords, API Keys

Unsure about a document? 🤔

If you're ever unsure about how to classify any data or document, **get in contact with your manager or IT Support Team** so we can perform a Data Classification Review.

8. REGIONAL AND INDUSTRY SPECIFIC REGULATIONS

Processing data that is subject to specific privacy or industry regulations requires a strict compliance review by IT prior to use. Using AI with regulated data (without specific legal agreements in place) can lead to serious legal penalties.

Please remember that most standard AI tools do not automatically meet these high standards. Many regulations require data to stay within a specific country or require strict audit logs that public AI tools simply do not provide. Just because a tool is popular or helpful does not mean it is compliant with the specific laws governing your industry.

You are responsible for adhering to the laws and regulations relevant to your specific role. If you have any questions regarding compliance, please speak to our IT or Legal Team.

9. CLIENT CONTRACT REQUIREMENTS

Our clients' contracts come first.

Before using AI on a client project, you must verify that the relevant Master Services Agreement (MSA) does not prohibit the use of AI.

If a contract forbids AI usage, **you must not use it**, regardless of the data classification.

10. MEETING RECORDERS AND EXTENSIONS

- **Automated Meeting Recorders:** Third-party AI bots (e.g., Otter.ai, Fireflies) are prohibited from joining meetings unless authorized by IT. If an unauthorized bot joins, the meeting host must remove it immediately.
- **Browser Extensions:** Installing browser extensions that use AI features is prohibited unless deployed by the IT Department. These extensions often require full read-access to web traffic, including private emails and banking portals.

11. MONITORING AND PRIVACY

➞ Company-provided AI accounts are company property.

The Company reserves the right to audit, monitor, and review all prompts, inputs, and outputs generated on these accounts to ensure compliance with this policy. Please remember that company **AI accounts are monitored and not private.** 👁

12. AI HALLUCINATIONS AND OUTPUT VERIFICATION

AI models frequently "hallucinate", and when they do, they confidently present incorrect information as fact.

You are required to **fact-check 100% of AI-generated claims** against a primary source.

<u>Never rely</u> on AI for:

- Legal Statutes or Case Law.
- Mathematical Calculations.
- Factual citations or historical dates.

If you make a business decision based on AI output, **you must validate the data first.**

13. INTELLECTUAL PROPERTY AND COPYRIGHT

AI-generated content occupies a complex legal gray area.

- 📃 **Copyright Risks:** Do not use AI to generate content that copies the distinct style of existing copyrighted works, or that deliberately reproduces protected trademarks.
- 📢 **Brand Representation:** Be cautious when using AI to generate photos, videos, or audio that represents our brand. AI often introduces subtle errors (e.g., misspelled logos, physical anomalies) that can damage our professional reputation.
- 💻 **Code Generation:** Using AI to generate software code or scripts is prohibited unless you are qualified to audit the code for security vulnerabilities. If you use AI for code, make sure it doesn't accidentally "borrow" open-source code that could cause legal issues.

14. AUTOMATION WORKFLOWS

Users are prohibited from creating automated workflows (e.g., via Zapier, Power Automate, Make.com) that automatically send company data to an AI API without prior IT review.

A wrongly set up automation can accidentally leak thousands of emails or files in minutes. Even if the AI tool is approved, the connection (API) **must be secured by IT.** 🔐

15. VOICE CLONING AND DEEPFAKES

The use of AI to clone, simulate, or mimic the voice 🗣️ or likeness of any human being (including staff, contractors, suppliers, or public figures) **is strictly prohibited** unless explicitly authorized in writing by Company Leadership.

This includes using "Text-to-Speech" tools that are trained on a specific individual's voice samples.

16. FINANCIAL VERIFICATION

Deepfake technology is now used to commit wire fraud.

Any urgent request for funds (wire transfers, gift cards, invoice payments) or credential changes received via voice, video, or email **requires secondary verification.**

If you get a call from the "CEO" asking for money, hang up. Call them back on their known internal phone number to **verify the request.**

17. AI-ASSISTED DECISIONS

AI tools lack human judgment, ethical reasoning, and real-world context.
They frequently "hallucinate" (invent facts) or rely on biased training data while sounding completely authoritative.

Relying on AI as the only decision-maker can lead to disastrous outcomes. A single unverified AI decision can result in wrongful termination lawsuits, flawed investment strategies, regulatory fines, and serious damage to our client relationships and brand reputation.

A human must review and approve ALL "AI-Assisted Decisions." This applies to any professional judgment, including but not limited to:

- Hiring and Termination decisions.
- Employee performance evaluations.
- Financial approvals.
- Strategic business planning.
- Professional Advice (Legal, Medical, Financial).

18. TRANSPARENCY AND AI-ASSISTED GENERATION

Transparency is key to maintaining client trust. 🤝

- **External Disclosure:** If AI is used to generate **any content** for a deliverable (e.g., a report, code module, image, or article), you must disclose the use of AI to the client, unless our contract states otherwise.
- **Internal Disclosure:** When submitting work to a manager, you must flag if the content was **"AI-Assisted Generation"** to ensure proper review.
- **Watermarking:** Where technically feasible, AI-generated images should keep their metadata or visible watermarks indicating their artificial origin.

19. MOBILE AND PERSONAL DEVICE USAGE (BYOD)

The use of AI apps on personal devices to work on company tasks is **prohibited.**

- You may not copy company emails, files, or chat logs into AI apps (e.g., the ChatGPT iOS/Android app) on a personal device.
- Mobile access to AI tools is only permitted via the company-managed Work Profile or approved apps installed by IT.

20. AI TRAINING REQUIREMENTS

Access is conditional on competence.

Access to company-provisioned AI tools is typically granted upon successful completion of **any required AI Training programs, including AI Security Awareness, AI Usability Training, and Ethics modules.** 🎥

The company reserves the right to revoke AI access for any employee who fails to complete required annual training.

21. VENDOR AND CONTRACTOR COMPLIANCE

Our security standards extend to our supply chain.

Contractors, Vendors, and Freelancers are required to use Company-Approved and Provisioned AI tools when working on Company data. Use of personal or free AI accounts by contractors is prohibited unless explicit written permission is granted by the IT Department.

All vendors must sign this AI Acceptable Use Policy as part of their onboarding process.

22. TERMINATION AND DATA RETENTION

We value the knowledge you create; thus your AI history belongs to the company. All prompts, inputs, and outputs generated using company-provisioned AI accounts are the exclusive property of The Company.

Upon termination of employment, IT will archive your AI account to ensure business continuity. **You may not delete, export, or transfer your AI chat history** to a personal account prior to departure.

23. ETHICS AND PROHIBITED CONTENT

AI tools may not be used to generate content that violates the company's Code of Conduct or Harassment Policy.

- **Prohibited Uses:** Users may not use AI to generate discriminatory, sexually explicit, hateful, or harassing content.
- **Malicious Use:** Users may not use AI to facilitate cyberattacks, create phishing emails, or generate malicious software.

24. SECURITY INTEGRITY ("JAILBREAKING")

Users are **strictly prohibited** from attempting to bypass the security filters, content moderation protocols, or safety guardrails of any AI tool (commonly known as "Jailbreaking" or "Prompt Injection"). Attempting to manipulate an AI tool to ignore its safety instructions is **a violation of this policy.**

25. INCIDENT REPORTING

If you accidentally input Restricted Data into an AI tool, or if you suspect an unauthorized bot has recorded a meeting, you must report it **immediately**. Self-reporting accidental errors is encouraged and allows for rapid fixing of the problem.

To report an issue, open an "Emergency Security Ticket" or call IT Support immediately.

26. POLICY REVIEW AND UPDATES

Due to the rapid pace of AI advancement, this policy is a living document.

This policy will be reviewed and updated by the company at least **every 6 months** (or upon the release of significant new AI capabilities) to ensure it addresses emerging risks.

Employees will be notified of any major updates to the Authorized Software list or security protocols. Continued use of company systems after an update means you agree to the new terms.

27. POLICY ENFORCEMENT AND ACKNOWLEDGMENT

We value a culture of trust and security. These guidelines are here to protect you, our clients, and the company's reputation. We understand that mistakes happen, but willful disregard for these safety measures—such as bypassing security controls or sharing sensitive data—is a serious issue.

If a violation is detected, we will investigate the circumstances. While accidental errors (especially those that are self-reported) are often treated as learning opportunities, deliberate violations or negligence will be met with appropriate disciplinary steps.

ACCEPTANCE

I have read and understood the Companies Artificial Intelligence Acceptable Use Policy. I agree to abide by the rules and responsibilities outlined above.

I understand that AI technology evolves rapidly, and I acknowledge that it is my responsibility to seek clarification from the IT Department or my manager if I am ever unsure about the safety of a specific tool or action. I will not assume a tool is safe just because it is publicly available.

Furthermore, I confirm that I understand my role in protecting company data. I agree to report any potential security risks, accidental data leaks, or suspicious activity immediately, understanding that early reporting helps protect the entire team.

EMPLOYEE NAME

EMPLOYEE SIGNATURE **DATE**

[APPENDIX A]: AUTHORIZED AI SOFTWARE LIST

[Keep this list separate so it can be updated without re-signing the whole policy]

The following tools have been vetted and are approved for use with **Internal Data:**

1. Microsoft Copilot Protected

All other tools are prohibited.