

The “Green Light” AI Usage Policy: Replace shadow AI with governed AI. Defines safe zones for innovation, telling employees exactly which tools to use and which data is permitted.

Instructions: Fill [BRACKETS] and issue to the entire organization to establish "License to Operate."




[COMPANY NAME] ACCEPTABLE USE POLICY

1. PURPOSE & SCOPE

This policy applies to all employees and contractors. Its goal is to empower you to leverage generative AI to eliminate drudgery and amplify creativity, provided it is done in accordance with our four Guiding Principles:

- **Value-Driven:** Use AI to advance strategic objectives, not just for novelty.
- **Human-Centered:** AI is a tool to augment your capabilities, not replace your judgment.
- **Secure:** We never compromise client privacy or company IP.
- **Accountable:** You are responsible for the final output, not the machine.

2. THE TOOL MATRIX (Which AI can I use?)

STATUS	TOOL CATEGORY	DATA RULES
 APPROVED	Enterprise Sandbox <i>(e.g., CCI AI Commons)</i>	Safe for Internal Data. You may upload internal docs, strategy, and non-sensitive data.
 RESTRICTED	Public LLMs <i>(e.g., Free ChatGPT/Gemini)</i>	Zero-Trust Environment. Use for general brainstorming <i>only</i> . NEVER input client names, code, financial data, or PII.
 PROHIBITED	Unvetted Tools <i>(e.g., Browser Extensions)</i>	Do Not Use. Any tool not explicitly approved by the CoE is blocked to prevent data scraping.

3. DATA SECURITY: THE "NO-FLY ZONE"

Regardless of the tool, the following data types are strictly prohibited from entry into any AI system without specific legal clearance:

- Sensitive Client Info:** PII (Personally Identifiable Information), PHI (Health), or private client records.
- Confidential Company IP:** Unpatented trade secrets, source code, or M&A strategy.
- Financial Data:** Non-public earnings or banking details.

4. THE HUMAN ACCOUNTABILITY CLAUSE

You are the Pilot. AI is the engine. You are required to:

1. **Fact-Check & Verify:** AI hallucinates. You must validate all outputs against trusted sources before use.
2. **Apply Judgment:** Do not accept AI drafts blindly. Edit, refine, and ensure the tone matches our brand.
3. **Disclose:** When producing external-facing content (reports, blogs), you must disclose if AI was a primary author.

5. INTELLECTUAL PROPERTY & OWNERSHIP

Treat AI deliverables as you would any other work product.

- **Company Ownership:** Any content, code, or strategy generated via company-approved AI tools during work hours is the exclusive property of [Company Name].
- **No Copyright Reliance:** Do not rely on AI-generated content for assets requiring strict copyright protection (e.g., logos, core trademarks) without Legal review, as AI output is currently difficult to copyright.

6. THE "VALUE LOOP" (Reporting Wins)

To scale what works, we must measure it.

- **Log Your Wins:** If an AI workflow saves you more than [**2 hours**] or generates a significant insight, you are required to log it in the [**AI Success Channel/Form**].
- **Share Your Prompts:** Don't hoard magic. Successful prompts should be submitted to the **Shared Library** so the whole team benefits.

7. COMPLIANCE & VIOLATIONS

Usage is a privilege. Violations of data security protocols will be addressed via standard disciplinary procedures. If you suspect a breach or have a question about a new tool, contact the **AI Center of Excellence (CoE)** immediately.

THE ROLLOUT COMMS PLAN

Don't just email the PDF. Use this 3-step sequence to drive adoption.

1. **The "Why" (CEO Email):** Announce the policy not as "Rules," but as "Permission."
 - *Subject: "Green Light: You are now authorized to use AI."*
2. **The "How" (Town Hall):** Demo the **Approved Sandbox** (Section 2) live. Show them where the "Safe Zone" is.
3. **The "What" (Manager Huddles):** Have managers review the **"No-Fly Zone"** (Section 3) with their teams to ensure specific data types are understood.