IMPLEMENTATION TIPS FOR THE BUSINESS OWNER

HOW TO ROLL THIS OUT:

1

THE "FIND AND REPLACE"

Simply swap [Company Name] with your business name, [Department Head/IT Support] with proper contact info, and update the date of the document. Add it to your existing AUP.

2

LEGAL CHECK

We are IT experts, not lawyers. While this policy covers the technical bases, always have your legal counsel review policy changes to ensure they align with local labor laws.

3

THE "AMNESTY" PERIOD

When you announce this, tell your team: "If you are already using tools like this, please tell us today. You won't be in trouble, but we need to secure them immediately." This prevents employees from hiding "Shadow IT" out of fear.

4

CONFIGURE YOUR TECH

A policy is just paper without enforcement. Contact Directive at 607-433-2200. We can configure your network and firewall settings to technically block many of these applications, ensuring that even if someone clicks a link by accident, your business stays safe.

directive

ADDENDUM TO ACCEPTABLE USE POLICY (AUP)

Subject: Usage of Autonomous AI Agents
Date: [DATE]
Applies To: All Employees, Contractors, and Third-Party Vendors

1. PURPOSE

[Company Name] recognizes the potential of Artificial Intelligence (AI) to improve efficiency and innovation. However, the use of Autonomous AI Agents—software that can act independently without constant human oversight—introduces significant security, privacy, and operational risks.

The purpose of this addendum is to clearly define the boundaries for using these tools to ensure the security of [Company Name]'s data, reputation, and infrastructure.

2. DEFINITION: WHAT IS AN AUTONOMOUS AI AGENT?

For the purposes of this policy, an Autonomous AI Agent is defined as:

Any AI-driven software, script, or platform capable of executing tasks, making decisions, or interacting with other systems, websites, or databases without continuous, direct human intervention for every specific action.

Distinction:

- **Standard AI (Allowed with caution):** Using ChatGPT, Gemini, or Copilot to draft an email is a standard AI task. You type a prompt, it gives a response. You are in control.
- **Autonomous Agent (Restricted):** Configuring an AI tool to automatically read your inbox, draft replies, and send them without you reviewing each one is an Autonomous Agent. Configuring an AI to browse the web, download files to a company server, or communicate on its own is an Autonomous Agent.

directive

3. PROHIBITED ACTIVITIES

To maintain the integrity of our network, the following activities are strictly prohibited unless explicit written approval has been granted via the process outlined in Section 4:

- **Unauthorized Installation:** Employees may not download, install, or execute any autonomous AI agent software (e.g., AutoGPT, BabyAGI, OpenClaw, Clawdbot, Moltbot, or browser-based automation extensions) on company-owned devices or personal devices connected to the company network.
- **System Integration & API Access:** Employees may not connect autonomous agents to [Company Name]'s internal systems, APIs, databases, or cloud storage environments (e.g., Microsoft 365, Sharepoint, CRM).
- **Credential Exposure:** Employees may not provide an autonomous agent with login credentials (usernames/passwords), API keys, or active session tokens that would allow the AI to masquerade as the employee.
- **Data Ingestion:** Employees may not input, upload, or expose Proprietary Information, Personally Identifiable Information (PII), or Protected Health Information (PHI) to any autonomous agent hosted on public or third-party servers.
- **Financial & Transactional Authority:** Employees may not authorize an AI agent to perform financial transactions, make purchases, or agree to Terms of Service on behalf of [Company Name].

4. RATIONALE: WHY THIS MATTERS

We are implementing this policy not to hinder innovation, but to prevent:

- **Data Leakage:** Autonomous agents often process data on external servers where we have no control over privacy.
- **"Hallucination" Risks:** AI agents can confidently make errors, potentially deleting data or sending incorrect information to clients.
- **Cybersecurity Threats:** Agents granted access to our network can be exploited by bad actors to deploy ransomware or steal data at machine speed.

5. APPROVAL PROCESS FOR LEGITIMATE USE CASES

If you believe you have a business case for using an Autonomous AI Agent to improve your workflow:

- **Do not proceed** without permission.
- Submit a request to [Department Head/IT Support] detailing the tool, the specific task it will perform, and the data it will access.
- The request will be reviewed by our IT Security team to ensure the tool is sandboxed and compliant with our security standards.

6. ENFORCEMENT

Violation of this policy poses a severe risk to [Company Name]. Employees found to have bypassed these security controls or engaged in prohibited activities regarding Autonomous AI Agents will be subject to disciplinary action, up to and including termination of employment and potential legal action.

ACKNOWLEDGMENT OF RECEIPT

I acknowledge that I have read and understand the Autonomous AI Agent Policy Addendum.

Employee Name: _____

Signature: _____

Date: _____