

P2. Acceptable Use of AI Policy

In accordance with ISO 42001 standards

Organization: Canopy IT Solutions

Owner: President

Confidentiality Level: External

Change History

2025-12-05	1.0	Bob Thompson	Initial Policy release

P.2.1 Purpose, Scope and Users

This policy defines the acceptable use, governance, and management of artificial intelligence employees and contractors of Canopy IT Solutions. It aims to protect the confidentiality, integrity, and availability of company and client data, and align with ISO 42001 standards

P.2.2 Implementation Method

- Employees are required to sign (physically or digitally) to confirm they’ve read and understood the policy on an annual basis
- Violations of this policy are submitted to the President or vCISO (automatically or via employee reporting) and tracked as security incidents

P.2.3 General Principles

Canopy IT Solutions provides employees with access to the Organization’s email system, RMM, computer networks, and other technology systems. Canopy IT takes a 3 tiered approach to ensuring the data in these systems is protected from external AI systems: Employee training and acceptable use, recommended AI settings, and data loss prevention.

- Employees are trained on AI use best practices and data protection. They are responsible for protecting company and client information from AI systems
- The IT infrastructure is configured to protect data from external AI systems
- Future item - Data Loss detection systems are in place to block and/or report on AI access to protected data

Acceptable Use of AI

- Use of AI should respect the rights and dignity of others. Any form of AI misuse that could harm individuals or groups is prohibited
- Use of deepfake technology to impersonate others is not allowed
- Employees should engage in discussion regarding the ethical implications of AI use and be aware of potential bias/limitations inherent with AI technology

- AI tools should be used to complement and enhance experience
- AI tools should be used for research, problem solving, and to supplement experience
- AI should only be used with approval from leadership
- The output of AI should be fully understood by the employee before use in the organization

Monitoring and Enforcement

- Any misuse of AI technology should be reported to leadership immediately
- Any misuse of AI technology will be subject to disciplinary action

P.2.4 Employee Training

Implementation Method

- Employees are required to complete a minimum of one Ironscales AI training module per quarter.
- Ironscales training is managed by the HR department.
- Training is mandatory, and tracked in the Ironscales training system

Criteria

- Date Released
- Time (25-30 minutes) or multiple five minute modules
- Current AI Security Trends

P.2.5 Best practices for workspace environments

Workspace environment settings are set to minimize AI access to data

- Settings are in place so 3rd party AI systems cannot read or analyze email messages
- Strict sharing settings are maintained so 3rd Party AI systems can't access documents or folders by default.
- Employees are only allowed to use their Google account to sign in to trusted apps, not just any app. For example, if someone tries to use their work Google account to log in to a new game or an unknown website, they won't be able to unless the company has approved that app. This helps keep your account safe from risky AI or unapproved apps

Evaluation of New AI platforms Will be Based on the Following Criteria

- Security Features
- Terms of Service
- Privacy Policy
- Vendor Reputation

						Scale 1 - 5			Low Risk (Score 1–6): Acceptable or monitor periodically.			Medium Risk (Score 8–12): Requires management attention and basic controls.			High Risk (Score 15–25) Requires remediation		
System	Asset Type	Function	Threat	Vulnerabilities	Frequency	Impact	Risk	Treatment Plan	Frequency	Impact	Risk	Frequency	Impact	Risk	Frequency	Impact	Risk
Kahn Academy Khanmigo	Cloud App	LMS	function	learning records	1	3	3	Risk Acceptance	1	3	3						
Power School / Powerbuddy	Cloud App	SMS	Application	student and family	5	2	10	Risk Acceptance...?	5	2	10						
Google GSuite	Cloud App	Productivity	PI exfiltration via AI	policy	5	1	5	Risk Acceptance	5	1	5						
Google Chrome	Web Browser	Web Browser	Unsecured AI extensions	access to confidential	4	4	16	extensions, only allow exceptions	4	1	4						
Non-approved AI apps	Cloud App	AI	of learning	Students have access	2	5	10	assignments during class	2	1	2						
Non-approved AI apps	Cloud App	AI	PI exfiltration	into AI	4	3	12	filter	4	1	4						