GenAI Policy

Andrew Galella
Josh Marquez
Mohsin Imtiaz
Judrianne Mahigne

Task

New technology is now capable of communicating and making content in ways comparable to humans. It's called *generative artificial intelligence (GenAI)*, and you can use it to excel in the workforce.

Your team has been engaged by one of the largest think tanks to help propose policy suggestions to help minimize the potential negative impact on the jobs, industry and personal data.

Overview

Analysis from multiple perspectives.

Inspiration from GDPR, CCPA, HIPAA, and other policies.

Perspectives:

AI Training

Time and Location Bounds

AI Reliance

Cybercrime

AI Training: Background

PII: Personally Identifiable Information

Two Sides of the Battle:

AI Companies	Privacy Advocates
AI data needs	Right to deletion
Hard to remove specific data points	Legal restrictions on using PII
Data removal can degrade performance	Major privacy risks if data is leaked

AI Training: Suggestions I

PII should never be used without an approved reason.

Instead, *anonymized data* must be used in its place.

If the use of PII is approved, the company needs:

- Clear written permission from Data Subject -

- Pseudonymization (Tokenization) -

- Encryption -

AI Training: Suggestions II

AI models should adhere to the concepts of PPML and XAI.

PPML: Privacy-Preserving Machine Learning

Data Confidentiality

Adversarial Robustness

Minimization of Data Usage

Resistance to Reverse Engineering

XAI: Explainable AI

- Clearly trackable, articulable, and demonstrable AI -

- Create transparency -

AI Training: Suggestions III

AI models should implement a policy of Zero Trust.

Zero Trust: Never trust, always verify.

Implementation:

- Require continuous authentication -

- Minimum permissions for minimum time -

- Only a certain few get access to resources and data -

Time & Location Boundaries: Overview

GenAI tools are restricted to only company-issued devices and secure environments.

Should be allowed only on:

- Company Networks
- VPS

GenAI should extend scrutiny and protections to branch sites.

Time & Location Boundaries

Environment and Access Control

- Should deploy within secure environments
- Must require VPN access for remote users
- Block personal devices, limit connection to company devices
- Enforce endpoint security policies

Time & Location Boundaries

Technical Controls:

- Implementation of VPS Devices
- Encrypt and **scrutinize** communications
    - We should monitor and secure the location of the use of communication channels (HTTPS, SSH) for all interactions.

Limitations on AI Reliance

Issue:

AI is reaching out into every job market.

AI is not infallible.

Limitations on AI Reliance

Risks of Overreliance:

- Job displacement, especially for vulnerable workers
- Legal Risks: Bias, Data Privacy Violations
- Loss of human oversight in critical decisions

Limitations on AI Reliance

We need to:

- Establish governance & oversight of AI use
- Train workers to adapt alongside AI
- Require human review in critical decisions

Limitations on AI Reliance

Implement Transparency Standards:

- Require explainable AI
- Track and document AI decision-making
- Regular audits to ensure fairness and accuracy

Generative AI Cybersecurity Policy

Acceptable Use Policy: Permitted Uses

- Utilizing GenAI for tasks like drafting non-sensitive executive report summaries.
- Generating code snippets for internal company tools such as scripts and/or manuals for proprietary appliances.
- Summarizing executive reports during routine business meetings.

Generative AI Cybersecurity Policy

Acceptable Use Policy: Prohibited Uses

- Inputting sensitive data (PII, confidential, and proprietary) into GenAI without proper approval.
- Using GenAI to create or distribute malicious software, phishing content, or any material intended for criminal activities.
- Employing GenAI outputs without proper legal written consent, especially in contexts that could go against company guidelines.

Generative AI Cybersecurity Policy

Preventive Policy Measures

- **Prompt and Output Review:**
  - Mandatory logs and analyze GenAI prompts and generated content to detect potentially non-compliant usage.
- **Network Segmentation:**
  - Isolate GenAI tools from systems processing sensitive data to reduce exposure risks.
- **Malicious Pattern Detection:**
  - Integrate threat detection systems that flag common patterns associated with AI-generated phishing, social engineering, or malware scripts.

Generative AI Cybersecurity Policy

Compliance and Enforcement

- **Verification of Internal Security:**
  - GenAI may not be used for official business use until the company's working infrastructure has been vetted by an authorized security auditor.
- **Auditing:**
  - Perform quarterly audits to assess compliance with the GenAI policy and identify areas for improvement.
- **Disciplinary Actions:**
  - Outline consequences for violations, which may include revocation of access privileges, disciplinary measures, or legal action, depending on the severity of the breach.

Conclusion

1. GenAI brings powerful benefits—but also serious risks.
2. Strong policies must ensure data privacy, transparency, and ethical use.
3. Zero Trust, environment controls, and human oversight are essential.
4. Acceptable use policies and regular audits promote accountability.
5. Our framework empowers innovation while protecting people and systems.

Thank You

Learn More

IBM

Crowdstrike

GFG - Data Anonymization

GDPR

NIST

Medium - PPML

Smarsh - GenAI and PII

ZScaler - AI and GDPR

aicpa-cima

trendmicro