

AI 201: Data Security, Privacy, Security On AI

Brian F. Tankersley, CPA.CITP, CGMA

K2 Enterprises

Copyright 2026, K2 Enterprises, LLC

Brian F. Tankersley, CPA.CITP, CGMA



brian@bftcpa.com
(865) 684-4707

- Has made presentations in 48 US States and three countries
- CPA, CITP, CGMA
- Top rated speaker with 30+ years of professional experience in accounting and technology
- Has published literally hundreds of reviews of products used by accounting professionals

Copyright 2026, K2 Enterprises, LLC

Brian Tankersley



- Has 20 beehives in two locations in East Tennessee



- Has five dogs: Lucy, Theo, Sammy. Lucinda, and Charlie





- Husband to Janette Burgin since 1993 (32 years!)

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Learning Objectives

Differentiate between AI security and privacy risks

List examples of key security and privacy risks associated with many of today's AI platforms

Identify best practices for mitigating the security and privacy risks associated with AI

Copyright 2026, K2 Enterprises, LLC

Major Topics



Major provisions of security and privacy policies



Key risks associated with using AI tools



Steps to take to mitigate AI security and privacy risks

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Safest AI Tools – Constitution/Indemnification

Safety

- Claude
- Copilot
- Perplexity AI
- ChatGPT
- Gemini
- Llama (Meta)

Popularity

- ChatGPT - 61% (14% in India)
- Copilot – 14%
- Gemini – 13%
- Perplexity AI – 6.2%
- Claude – 3.2% (80% business)
- All others below 1%

Copyright 2026, K2 Enterprises, LLC

Are There Dangers With AI? ***Absolutely***!

Biased Outputs	Copyright infringement	Data privacy
Data security	Deepfakes	Hallucinations

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Are There Dangers With AI? ***Absolutely***!



Biased Outputs	Copyright infringement	Data privacy
Data security	Deepfakes	Hallucinations

Copyright 2026, K2 Enterprises, LLC

AI And Copyright



- The consensus from all of the engines is that AI-only output is in the public domain with no owner, while AI-assisted work may be copyrightable if human input is perceptible
- Major AI engines like Claude, Gemini, ChatGPT, and Perplexity all transfer ownership of the generated content to the user
- The statutes in other countries handle copyright differently – one notable exception is the UK's 50 year copyright on AI-generated content

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AI And Copyright

Platform	Do they claim your output?	Can you use it commercially?	Will they protect you if sued?
OpenAI	❌ No, assigned to you	Yes	Yes (API / Business tiers only)
Anthropic	❌ No, assigned to you	Yes	Yes (Commercial / API tiers only)
Google	❌ No, treated as your data	Yes	Yes (Cloud / Workspace customers)
Perplexity	❌ No, assigned to you	Yes	❌ No (User assumes third-party web risks)

Copyright 2026, K2 Enterprises, LLC

Training AI With Copyrighted Data

- This is an area where the law is still evolving – it is NOT settled law at this time
- In the US, this is governed by the four pillars of the Fair Use Doctrine (17 USC §107)
  - **Purpose and character of use** — Is it transformative? Commercial?
  - **Nature of the copyrighted work** — Is it factual or creative?
  - **Amount used** — How much of the original was ingested?
  - **Effect on the market** — Does it harm the copyright holder's market

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Training AI With Copyrighted Data

- Some legal scholars/observers have identified three emerging rules in the precedents:
  - Legally obtained data can be fair use when training is genuinely transformative and market harm is speculative
  - Pirated or stolen training data is never protected — Bartz v. Anthropic specifically carved out that Anthropic's use of pirated books was not excused, even where fair use otherwise applied
  - Competing directly with the source destroys the fair use defense because market harm becomes concrete and obvious

Copyright 2026, K2 Enterprises, LLC

Copyright Infringement

Who owns the copyright to materials generated by AI?

Response, Per ChatGPT	Response, Per Gemini
Generally, the entity or individual that creates the AI-generated content is considered the copyright owner. However, this may vary based on jurisdiction and specific contractual agreements	*In the United States, the Copyright Office has stated that it will not register works that were created by an autonomous AI tool. This means that, under current US law, AI-generated works are either in the public domain or they are derivative works of the materials that the AI was trained on*

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Copyright Infringement



New York Times Has Sued MSFT & OpenAI!

- In December, NYT sued Microsoft and ChatGPT's parent company, OpenAI
- The Times alleges "*mass copyright infringement*"
- The Times continues with *"These tools were built with and continue to use independent journalism and content that is only available because we and our peers reported, edited, and fact-checked it at high cost and with considerable expertise"*
- One example provided by the Times OpenAI's software producing almost identical text to a Times article about predatory lending practices in New York City's taxi industry

Copyright 2026, K2 Enterprises, LLC

Data Privacy



- Consider the type of data you might upload into an AI tool or platform…how comfortable are you that sensitive data remains private and not identifiable back to an individual, a client, or an organization?
- Other issues include
  - Is there informed consent about collection and use
  - The threat of exposing sensitive data through a breach or attack
  - Lack of transparency regarding using an individual's or organization's data

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

EU: General Data Protection Regulation

Overview

- Cornerstone of EU data privacy law since 2018
- Influenced privacy laws globally — the “Brussels Effect”

Core Focus Areas

- Transparency in how personal data is collected and used
- Accountability of organizations handling data
- Individual rights over personal information



Copyright 2026, K2 Enterprises, LLC

EU: Artificial Intelligence Act

Scope - Regulates AI systems based on risk levels to fundamental rights, health, and safety

Prohibited High-Risk Applications

- Social scoring systems
- Real-time biometric identification in public spaces

Timeline – Began phasing-in August 2024**;** Full compliance expected by August 2026

Requirements for High-Risk AI

- Risk management systems
- Transparency measures
- Data governance practices
- Human oversight

Upcoming Initiatives

- AI literacy programs
- Codes of Practice for General Purpose AI (May 2025)
- Governance for systemic-risk AI models

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

EU: DORA and GDPR Simplification

Digital Operational Resilience Act (DORA)

- Complements GDPR and the AI Act
- Focuses on resilience in digital operations, especially financial services
- Ensures robust cybersecurity and incident reporting

GDPR Simplification Proposal (May 2025)

- Targets small mid-cap enterprises (SMCs)
- SMCs defined as <750 employees, balance sheet <€129M, turnover <€150M
- Extends derogations from record-keeping obligations (Article 30 GDPR)
- Reduces administrative burden while maintaining data protection standards
- Encourages tailored codes of conduct and certification mechanisms

Copyright 2026, K2 Enterprises, LLC

EU: New Procedural Rules for GDPR Enforcement

- Adopted May 2025
- Improves enforcement of large, cross-border cases
- Designed to make GDPR enforcement faster and more effective
- **Why It Matters**
  - Streamlines coordination between national data protection authorities
  - Reduces delays in resolving multi-jurisdiction complaints
  - Strengthens consistency of enforcement outcomes across the EU

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Canada: Federal Privacy Laws

- **Privacy Act**
- Governs how federal government institutions collect, use, and disclose personal information
- Applies to federal departments, agencies, and Crown corporations
- **PIPEDA -** Personal Information Protection and Electronic Documents Act
- Applies to private-sector organizations engaged in commercial activities
- Covers collection, use, and disclosure of personal information during commercial activities
- Enforced by the Office of the Privacy Commissioner of Canada
- Bill C-27 is dead (would have provided significant updates to both statutes; no major legislation proposed at this time)



Copyright 2026, K2 Enterprises, LLC

Canada: Health and Provincial Privacy Statutes

- **Health Sector Privacy**
- Personal Health Information Protection Act (PHIPA) — Ontario
- Health Information Act (HIA) — Alberta
- Act Respecting Health Services and Social Services (ARHSSS) — Quebec
- Govern handling of personal health information by healthcare providers

- **Provincial Private-Sector Laws -** Deemed substantially similar to PIPEDA:
- Quebec: Act Respecting the Protection of Personal Information in the Private Sector (amended by Law 25 in 2023)
- British Columbia: Personal Information Protection Act (BC PIPA)
- Alberta: Personal Information Protection Act (AB PIPA)

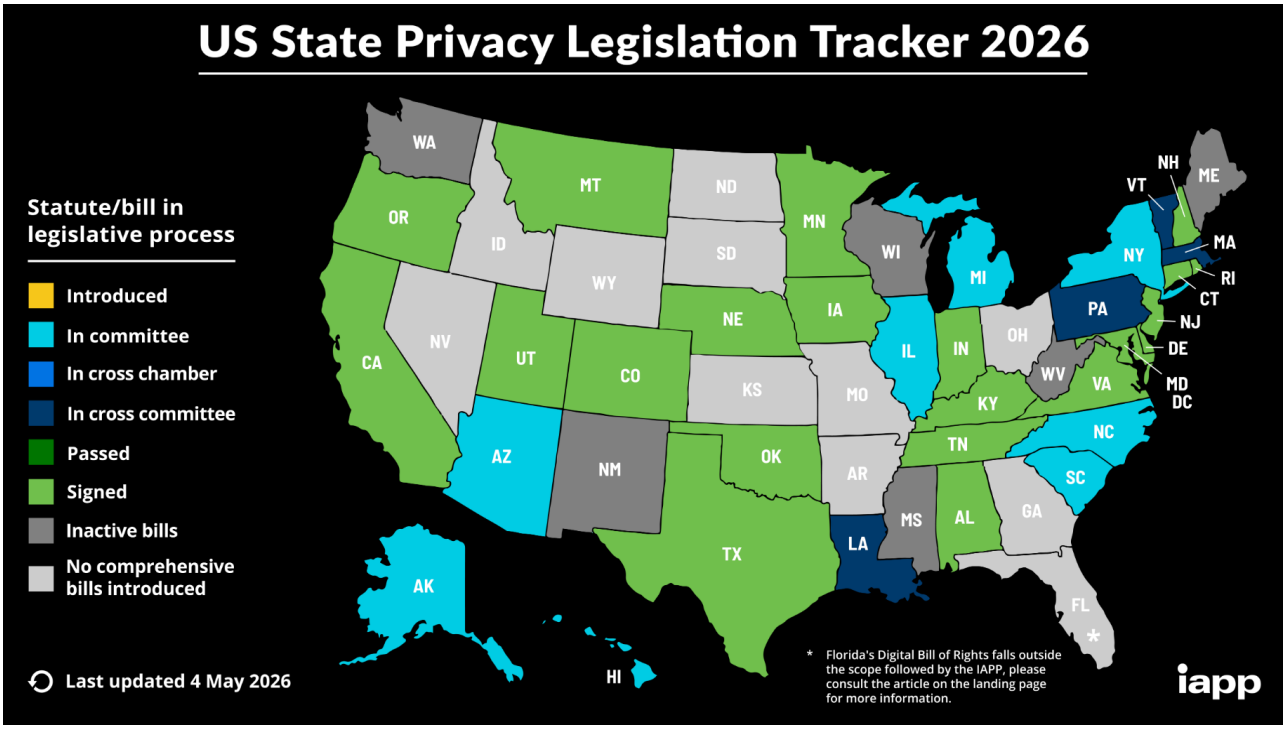
Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Canada: Employment and Sector-Specific Laws

- **Employment Privacy**
  - Employment-related privacy protections may be embedded in labor codes
  - Sector-specific regulations also apply depending on industry
  - Coverage and rights vary by jurisdiction and employer type
- **Public Sector and Education**
  - Provinces have additional rules for public bodies
  - Educational institutions are subject to dedicated privacy frameworks
  - These supplement federal and provincial general privacy laws

Copyright 2026, K2 Enterprises, LLC



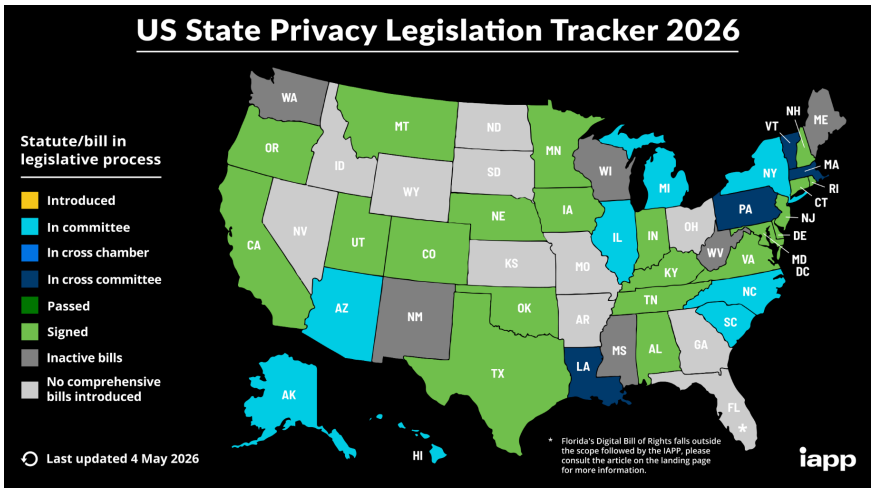
Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

State Privacy Regulations

1. California Consumer Privacy Act (Oct 1, 2020, amended Jan 1, 2023)
2. Colorado Privacy Act (Jul 1, 2023)
3. Connecticut Personal Data Privacy and Online Monitoring Act (Jul 1, 2023)
4. Delaware Personal Data Privacy Act (Jan 1, 2025)
5. Indiana Consumer Data Protection Act (Jan 1, 2026)
6. Iowa Consumer Data Protection Act (Jan 1, 2025)
7. Kentucky Consumer Data Protection Act (Jan 1, 2026)
8. Maryland Online Data Privacy Act (Oct 1, 2025)
9. Minnesota Consumer Data Privacy Act (Jul 31, 2025)
10. Montana Consumer Data Privacy Act (Oct 1, 2024)
11. Nebraska Data Privacy Act (Jan 1, 2025)
12. New Hampshire SB 255 (Jan 1, 2025)
13. New Jersey SB 332 (Jan 15, 2025)
14. Oregon Consumer Privacy Act (Jul 1, 2024)
15. Rhode Island Data Transparency and Privacy Protection Act (Jan 1, 2026)
16. Tennessee Information Protection Act (Jul 1, 2025)
17. Texas Data Privacy and Security Act (Jul 1, 2024)
18. Utah Consumer Privacy Act (Dec 31, 2023)
19. Virginia Consumer Data Protection Act (Jan 1, 2023)

Copyright 2026, K2 Enterprises, LLC

US State Privacy Legislation 2026



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

UT Digital Choice Act HB418 7/1/26

- Utah’s groundbreaking new Digital Choice Act will finally give people agency over their data on social media
- Under the act, individuals will be able to use open-source protocols to seamlessly move their content and relationships to new apps if they are unhappy with the experience on a social media site. It aims to challenge Big Tech's monopolistic practices and foster competition in the digital ecosystem. The law reflects growing public sentiment for greater control over personal data and targeted advertising, marking a significant step toward a more user-centric internet. Provisions:
  1. Complete Data Portability
  2. Right to Deletion
  3. Enforces Interoperability

Copyright 2026, K2 Enterprises, LLC

CA SB 53 Transparency In Frontier Artificial Intelligence Act (TFAIA)

- California Governor Gavin Newsom signed SB 53 on 9/30/25, the nation’s first law placing guardrails on frontier AI
- Newsom described it as installing “commonsense guardrails” to build public trust without stifling innovation. Anthropic, Stanford, UC Berkley, and others endorsed
- The new law applies to frontier AI models, or the most advanced systems with significant capabilities and risks. What SB53 does:
  1. **Transparency:** Requires major AI developers to publish a framework showing how they follow national and international standards, making their practices visible to the public
  2. **Innovation:** Establishes CalCompute, a state-backed public computing consortium to support safe, equitable AI research
  3. **Safety:** Sets up a system for companies and the public to report critical AI safety incidents directly to California’s Office of Emergency Services
  4. **Accountability:** Protects whistleblowers who expose serious risks from frontier models and imposes civil penalties for noncompliance, enforceable by the attorney general
  5. **Responsiveness:** Directs the Department of Technology to recommend annual updates, so the law keeps pace with rapid advances and international standards

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Data Security

- Like other large caches of data, the data stored in AI tools and platforms can present an inviting target because of the private nature of the data
- Additionally, a general lack of human oversight can increase the vulnerability of the data
- Moreover, the complexity of AI systems presents challenges concerning storing and protecting sensitive data
- In fact, as reported on 11/10/23, Microsoft temporarily blocked team members from using ChatGPT due to security concerns

Copyright 2026, K2 Enterprises, LLC

President Trump Signs AI Executive Order: "Promoting Advanced Artificial Intelligence Innovation and Security"

Key Message: *The Administration's first major AI security directive balances innovation with national security — emphasizing voluntary industry collaboration over mandatory regulation.*

- Builds on the July 2025 AI Action Plan (90+ policy recommendations)
- Targets frontier AI models and critical infrastructure cybersecurity
- Accompanied by a National Security Presidential Memorandum on AI (June 5, 2026)
- Does NOT create mandatory licensing, pre-clearance, or permitting requirements for AI developers

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Three Core Directives of Exec Order

Strengthen Federal Cybersecurity (30 Day/by July 2)

- CISA must issue Binding Operational Directives to accelerate cyber defense of civilian federal systems
- AI-enabled defensive tools expanded to state/local governments, rural hospitals, community banks, and utilities
- Treasury to establish a voluntary "AI Cybersecurity Clearinghouse" for vulnerability scanning and patch coordination
- OPM to expand hiring pathways for US Tech Force cybersecurity specialists (60-day deadline)

Frontier Model Pre-Release Framework (60 Days / by Aug 1)

- NSA leads a classified benchmarking process to define "covered frontier models"
- Developers may voluntarily provide government access to covered models up to 30 days before release to "trusted partners"
- IP and confidentiality protections required; specific terms still to be developed
- Key terms ("covered frontier model," "trusted partners") remain undefined pending agency guidance

Enforce AI-Enabled Cybercrime Laws (Immediate)

- Attorney General directed to prioritize prosecution under existing federal statutes
- Targets: unauthorized computer access, wire fraud, identity fraud enabled by AI
- Includes AI agents used to unlawfully access data for criminal purposes
- No new laws created — enforcement of existing statutes (CFAA, 18 U.S.C. §§ 1028, 1343)

Copyright 2026, K2 Enterprises, LLC

What This Means for Your Organization

- **For AI Developers / Technology Companies:**
- Determine whether your models may qualify as "covered frontier models" — engage agencies after August 1 guidance is issued
- Evaluate voluntary participation in the pre-release framework; weigh IP risk against relationship-building opportunity
- Ensure AI agents have robust access controls, permission scoping, and audit logging to limit criminal liability exposure

- **For Critical Infrastructure Operators (including financial institutions):**
- Monitor the Treasury-led AI Cybersecurity Clearinghouse for vulnerability intelligence opportunities
- Assess data-sharing risks before participating (FOIA exposure, enforcement use of disclosed vulnerabilities)
- Expand cybersecurity posture to meet forthcoming CISA Binding Operational Directives

Key Dates to Watch:

- July 2, 2026 — CISA directives and cybersecurity tool expansion due
- July 2, 2026 — AI Cybersecurity Clearinghouse formation due
- August 1, 2026 — Classified benchmarking process and voluntary pre-release framework due
- August 1, 2026 — OPM cybersecurity hiring pathway expansion due

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Claude Fable 5 Withdrawn

- On June 12th, the US Commerce Department invoked provisions of the International Trade in Arms Act (ITAR) to restrict the use of Claude Fable 5 to US citizens only
- Fable (f/k/a Mythos) had incorporated significant guardrails surrounding its use to solve biological and nuclear weapons problems, but it was not enough for USDOC
- Anthropic pulled the model on 6/12/2026, negotiations are ongoing at this time



A\

Statement on the US government directive to suspend access to Fable 5 and Mythos 5

Jun 12, 2026

The US government, citing national security authorities, has issued an export control directive to suspend all access to Fable 5 and Mythos 5 by any foreign national, whether inside or outside the United States, including foreign national Anthropic employees. The net effect of this order is that we must abruptly disable Fable 5 and Mythos 5 for **all** our customers to ensure compliance. **Access to all other Anthropic models will not be affected.**

Copyright 2026, K2 Enterprises, LLC

Understand what you're getting into with generative AI

SOFTWARE LICENSES AND PRIVACY POLICIES

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Just Another Battle In A Long War...



- Historically, software licensing and use policies have been a problem for parties on both sides of the fence
- That hasn't changed with AI, and likely will not change soon
- On the developer side, there is an incentive to get as much quality data as possible into the LLMs, while simultaneously building up the subscriber base
- However, on the end-user side, we should not share data that is private/sensitive with the outside world
  - Do you ***really*** want to upload your tax return to an AI platform?

Copyright 2026, K2 Enterprises, LLC

Add AI And It Gets Complicated



- Software licensing and data usage policies have always been hard to understand – even with search engines
- Now, consider the impact of Artificial Intelligence (AI) when added to the mix
- Could creating a prompt asking for tax advice expose your personal data or that of a client?
- Could uploading financial data for a privately-held company to an AI platform cause that data to leak?
- Can we trust what the AI companies are telling us about data security and privacy?

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Understanding Licenses Is Critical



- To better understand the risks associated with privacy and AI, we need to **READ** and **UNDERSTAND** the major documents associated with the application
- Two of the key documents associated with your rights/license to use software or cloud-based services include:
  - End User License Agreement (EULA) a/k/a Terms of Service (ToS)
  - Privacy Policy

Copyright 2026, K2 Enterprises, LLC

ChatGPT's Terms Of Use Key Points



- Must be at least 13 and, if under 18, have parental consent
- Cannot use ChatGPT for “illegal, harmful, or abusive” activity, including infringing upon or violating anyone’s rights
- You cannot represent that results are human-generated
- You retain ownership rights to your inputs and outputs
- ChatGPT can use your content to “provide, maintain, develop, and improve our services”
- You can opt out of ChatGPT using your data to train ChatGPT

https://openai.com/policies/terms-of-use/

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Data Is Used To Train LLMs

Information that is publicly available on the internet

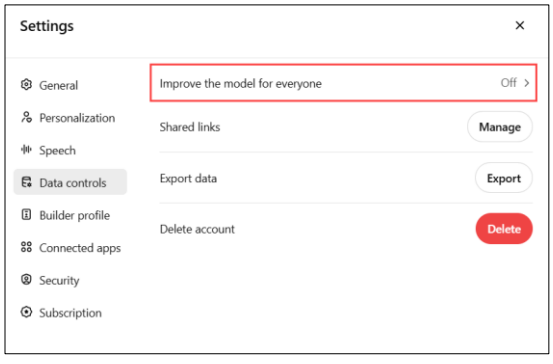
Information that we partner with third parties to access and use

Information that our users or human trainers and researchers provide or generate

Copyright 2026, K2 Enterprises, LLC

To Opt-Out Of ChatGPT's Training…

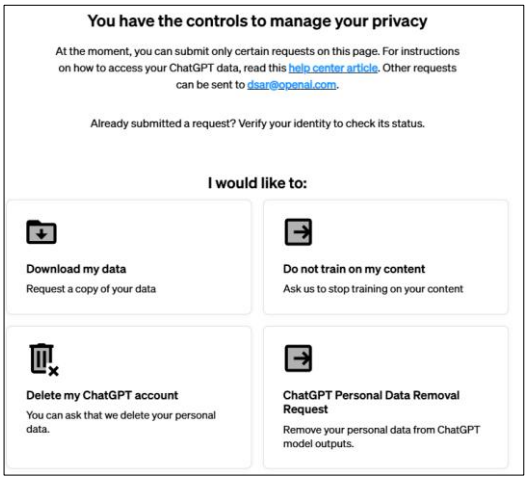
- Visit ChatGPT's **Settings**
- Next, click **Data controls**
- Finally, turn off the **Improve the model for everyone** option as shown on the right
- It's a good idea to review all the other settings also to ensure they align with your expectations and needs



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

ChatGPT's Privacy Request Portal



- You can find the **Privacy Request Portal** at https://k2e.fyi/OAIPrivacy or by using the QR code below

Copyright 2026, K2 Enterprises, LLC

Privacy Policy

- Document which discusses a company's privacy policy, including data like
  - What data is gathered from you
  - How your information will be used
  - The purpose of gathering that data and how your data may be used
  - When your data will be disclosed to others, including sensitive personal data and information
    - Not always specific on with whom it will be shared
  - Security policies and procedures
- Consider ChatGPT's Privacy Policy

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Acceptable Use Policy



- Just as the EULA/ToS, and privacy policy spell out the rights and responsibilities of both parties in a relationship between an end user and a software company, an Acceptable Use Policy (AUP) governs the acceptable use of the organization's technology hardware, software, and data by its employees and contractors
- Although acceptable use policies are not required by law, they help both employees and companies properly set expectations about how these tools will be used (and how they will NOT be used) so all parties know their rights and responsibilities

Copyright 2026, K2 Enterprises, LLC

Acceptable Use Policy Defines



Ownership and general use of technology
Security and handling confidential information
Types of unacceptable use of systems
E-mail and communication guidelines
Blogging and social media
Consequences for violation of these policies

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Potential Harms From AI Systems

Harm to People	Harm to an Organization	Harm to an Ecosystem
• Individual: Harm to a person's civil liberties, rights, physical or psychological safety, or economic opportunity.	• Harm to an organization's business operations.	• Harm to interconnected and interdependent elements and resources.
• Group/Community: Harm to a group such as discrimination against a population sub-group.	• Harm to an organization from security breaches or monetary loss.	• Harm to the global financial system, supply chain, or interrelated systems.
• Societal: Harm to democratic participation or educational access.	• Harm to an organization's reputation.	• Harm to natural resources, the environment, and planet.

Source: "Artificial Intelligence Risk Management Framework" (AI 100.1) by US National Institutes for Standards and Technology (NIST)

Copyright 2026, K2 Enterprises, LLC

SO, WHAT ARE THE AI COMPANIES SAYING?

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

ChatGPT Data Concerns



- OpenAI (ChatGPT's parent company) collects:
  - IP address, location, browser type, date/time, length of session, device name, and operating system
  - Uses cookies to track browsing activities both in chat window and site
  - Records complete transcripts of your prompts and conversations
  - ChatGPT reserves the right record any data you upload, such as an Excel file or a set of financial statements
- As discussed previously, to enhance security and privacy, consider opting out of model improvement and deleting your chat history

Copyright 2026, K2 Enterprises, LLC

Gemini Concerns



- Google publicly stated that Gemini collects the following information about your use of Gemini
  - Conversations, locations, feedback, and usage info
- Regarding accessing to your Gemini conversations, Google says the following: *We take your privacy seriously, and we do not sell your personal information to anyone. To help Gemini improve while protecting your privacy, we select a subset of conversations and use automated tools to help remove user-identifying information (such as email addresses and phone numbers).*

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Gemini Concerns



- Google goes on to state: *Please don't enter confidential information in your conversations or any data you wouldn't want a reviewer to see or Google to use to improve our products, services, and machine-learning technologies.*
- *Gemini Apps conversations that have been reviewed by human reviewers are not deleted when you delete your Gemini Apps activity because they are kept separately and are not connected to your Google Account. Instead, they are retained for up to three years.*

Copyright 2026, K2 Enterprises, LLC



MICROSOFT'S COPILOT OFFERING IS A BIT DIFFERENT

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Some of Microsoft's AI Copilots

Name	Products	Monthly Cost	Enterprise Data Protection Included?
Copilot for MS 365 (Business/Enterprise)	Microsoft 365 apps (Word, Excel, PowerPoint, Outlook, Teams)	$30 per user	**Yes**
Copilot in Windows (Bing Chat)	Windows OS	Free	Not for home users, included with most business/enterprise O365/M365 plans
Copilot Pro for Individuals	Advanced features on top of standard Copilot, plus integration with home Microsoft 365 apps	$20/user/mo.	Not specified
Copilot for Security	Microsoft's cybersecurity products	Consumption-based fee - $4/hour	Not specified
Designer for Copilot	Image creation and editing	Not available	No
Copilot GPTs and Azure AI Studio	Custom generative AI assistants and solutions	Not specified	Not specified

Copyright 2026, K2 Enterprises, LLC

Enterprise Data Protection

- Data is not used to train AI models
  - Prompts and responses in Copilot (when EDP is enabled) are not retained or used to train Microsoft's underlying AI models, helping protect sensitive business information.
- Microsoft has no "eyes-on" access to your data
  - Microsoft does not access or review your Copilot prompts and responses, ensuring organizational confidentiality is preserved. Strong encryption protects all data
- Data is encrypted both in transit and at rest, using enterprise-grade security standards to protect information end-to-end.

Copyright 2026, K2 Enterprises, LLC

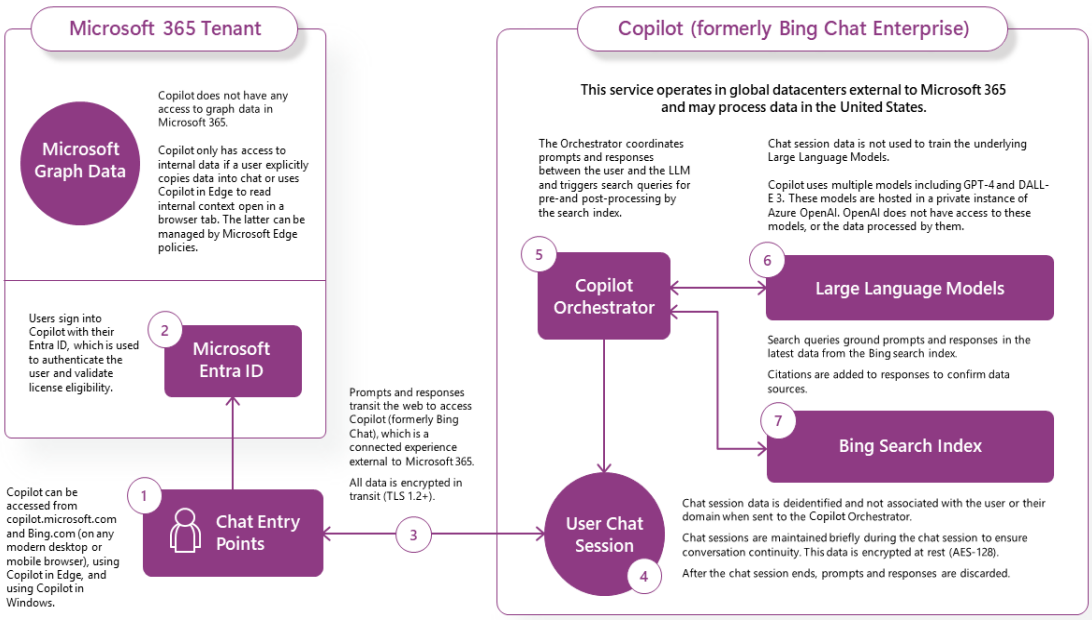
Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Enterprise Data Protection

- Access is controlled via Microsoft Entra ID
  - Only authorized users within the organization can access Copilot with EDP, enforced through identity and access management (Entra ID).
  - No targeted advertising based on work data
- Copilot does not use your organizational prompts, responses, or identity to target ads or personalize advertising, maintaining a strict separation between work data and commercial use.

Copyright 2026, K2 Enterprises, LLC

Copilots and Data Protection



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

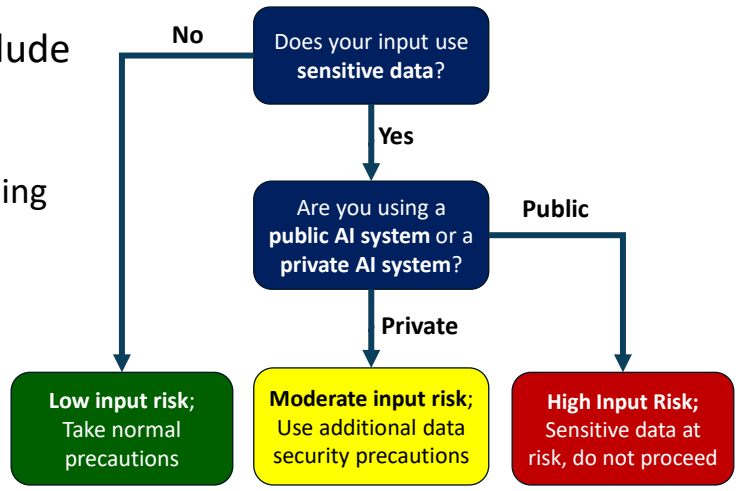
Three Types Of GenAI Risk

Input risks	Output risks	System risks
• The risks associated with exposing your proprietary data to an AI system and that data becoming compromised, which results in unauthorized disclosure of confidential information	• The risks that the outputs from the AI model will be low quality, inaccurate, or incomplete and the models lose their integrity based on including an unacceptable number of erroneous data points	• Risks associated with the servers hosting the AI system being compromised and the data model needs to be recovered from backups

Copyright 2026, K2 Enterprises, LLC

Gen AI Input Risk Decision Tree

- Types of input attacks include attempts to:
  - Crash AI model
  - Exfiltrate memorized training data



Source: "Address Security & Privacy Risks for Generative AI" by InfoTech Research Group

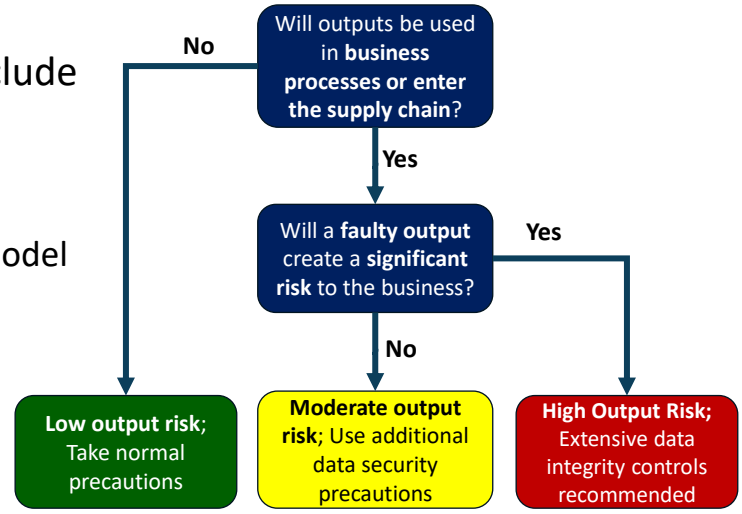
Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Gen AI Output Risk Decision Tree

Types of output attacks include attempts to

- Data poisoning that could corrupt AI output
- Weaponization of an AI model
- Sponging to slow down processing speed of AI model

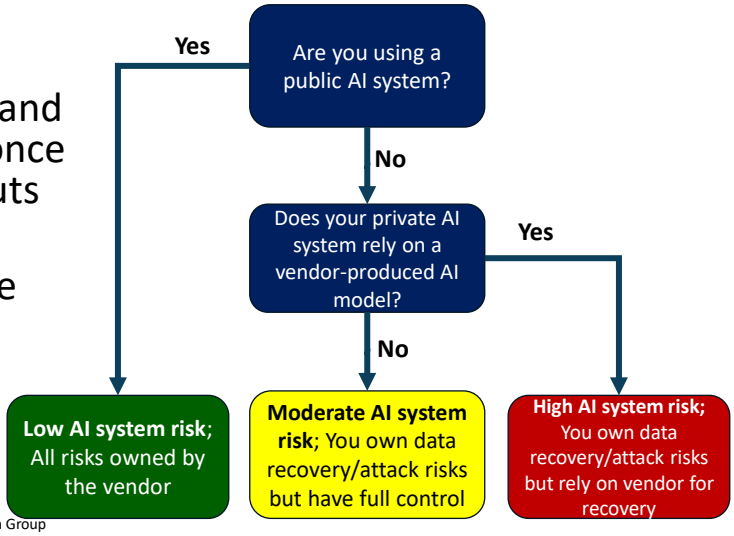


Source: "Address Security & Privacy Risks for Generative AI" by InfoTech Research Group

Copyright 2026, K2 Enterprises, LLC

Gen AI System Risk Decision Tree

- Public AI systems like ChatGPT, Google Gemini, and Bing chat are developed once and trained based on inputs from many users
- Private AI systems must be trained, managed, and maintained by employees using internal organization resources



Source: "Address Security & Privacy Risks for Generative AI" by InfoTech Research Group

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

*"Florida Man Accused Of Posing As Elon Musk, Defrauding Elderly Woman Of $250K", **Fox Business** 11/21/2024*
*"Arup Lost $25mn In Hong Kong Deepfake Video Conference Scam", **Financial Times** 5/16/2024*
*"British Engineering Giant Arup Revealed As $25 Million Deepfake Scam Victim", **CNN** 5/17/2024*

DEEPFAKES: SEEING IS NOT BELIEVING

Copyright 2026, K2 Enterprises, LLC

THIS IS NOT ELON MUSK!!! IT IS FAKE!



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Happened: Elon Impersonated

- Elon Musk has been impersonated many times due to his wealth and his status in society
- ANYONE who appears in videos online can be duplicated with varying levels of success

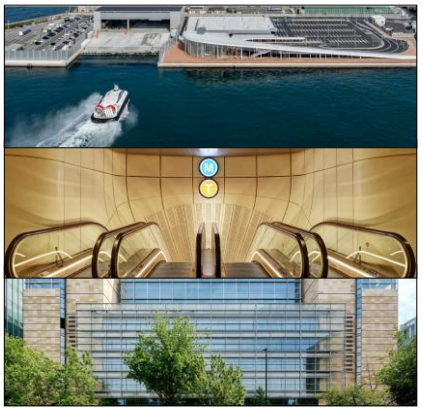


Copyright 2026, K2 Enterprises, LLC

What Happened: Arup Impersonation

- Fraudsters created a digitally cloned version of a senior manager at global engineering and design firm Arup
- This "clone" was used to order financial transfers totaling approximately HK$ 200 million during a video meeting
  - HK$ 200 MM is approximately $25MM USD or $35MM CAD
- Arup executed all the 15 requested transactions, resulting in the loss of the transferred funds

ARUP



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Ad Firm WPP's CEO Falls For Deepfake

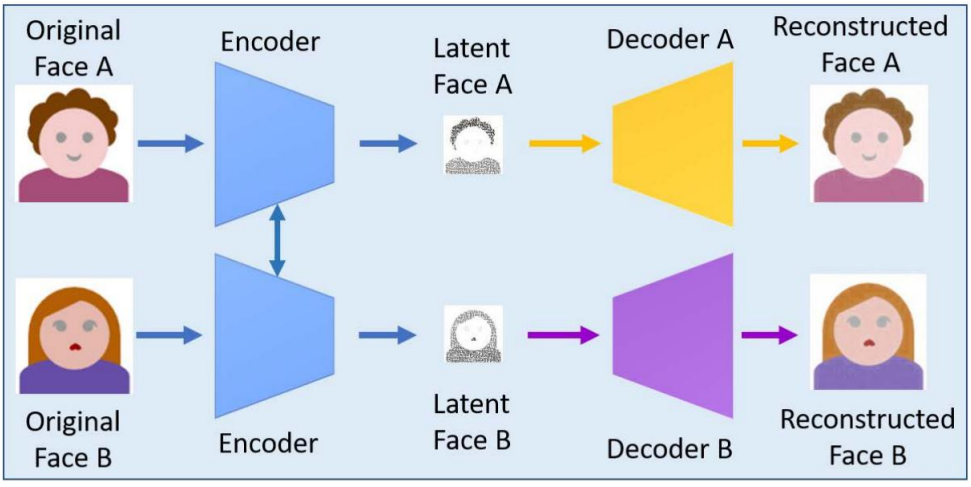
- In May 2024, global advertising firm WPP CEO Mark Read fell victim to a scam that sought to steal personal data and assets of executives
- The CEO saw his voice cloned and likeness stolen by fraudsters, and discovered a fake WhatsApp account under his name
- The WhatsApp account was used to set up a virtual meeting, where fraudsters:
  - played fake video as if it was live video of the CEO participating in the meeting and
  - impersonated Read in the chat messages of the meeting



Mark Read
CEO, WPP

Copyright 2026, K2 Enterprises, LLC

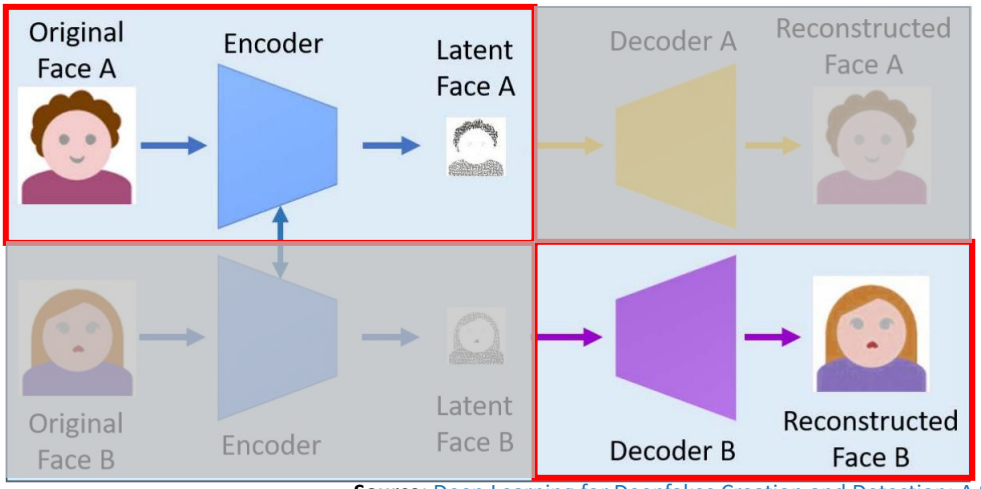
How Deepfake Image Creation Works



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

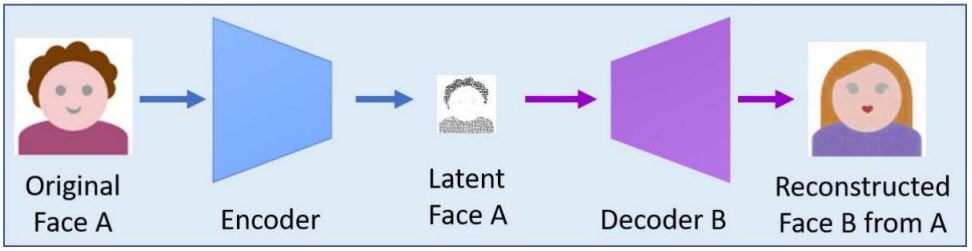
How Deepfake Image Creation Works



Source: Deep Learning for Deepfakes Creation and Detection: A Survey (arxiv.org)

Copyright 2026, K2 Enterprises, LLC

How Deepfake Image Creation Works



Soured: Deep Learning for Deepfakes Creation and Detection: A Survey (arxiv.org)

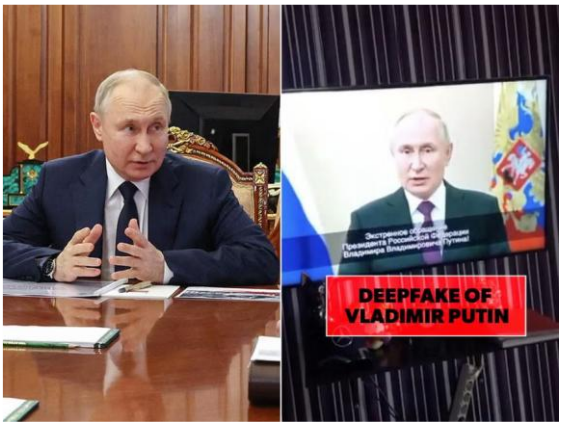
Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Are Deepfakes?

Deepfakes are AI-generated, highly realistic synthetic media that can be abused to:

- Threaten an organization's brand
- Impersonate leaders and financial officers
- Enable access to networks, communications, and sensitive information



Source: US NSA/FBI/CSIS Cybersecurity Information Sheet: Contextualizing Deepfake Threats to Organizations

Copyright 2026, K2 Enterprises, LLC



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Summary And Wrap Up



- Proactively manage the security and privacy settings in the AI platforms that you use
- Never enter or upload private or sensitive data into your generative AI prompts
  - Scrub names, SSN's, account numbers, etc. from your data before uploading it to a generative AI tool
- Train your team members on how to use these tools safely and securely…remember the survival of your business may depend upon it!

Copyright 2026, K2 Enterprises, LLC



Questions?

THANK YOU FOR ATTENDING

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.