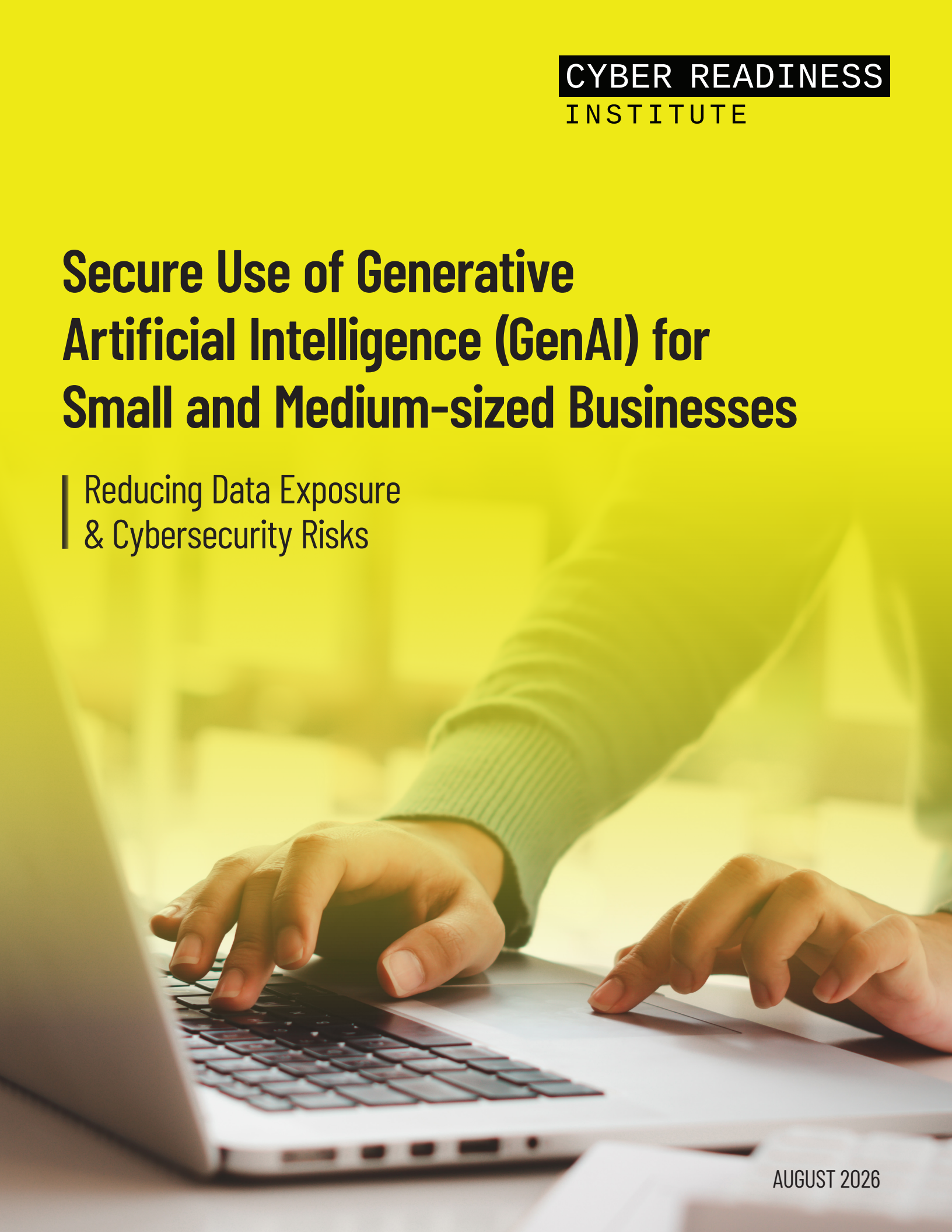
CYBER READINESS
INSTITUTE

Secure Use of Generative Artificial Intelligence (GenAI) for Small and Medium-sized Businesses

Reducing Data Exposure & Cybersecurity Risks



AUGUST 2026

Introduction

Artificial Intelligence (AI) is reshaping business operations by enabling greater efficiency, improved analytics, and enhanced customer engagement. At the same time, it introduces new cybersecurity risks, including data exposure, improper use of sensitive information, and exploitation by cybercriminals.

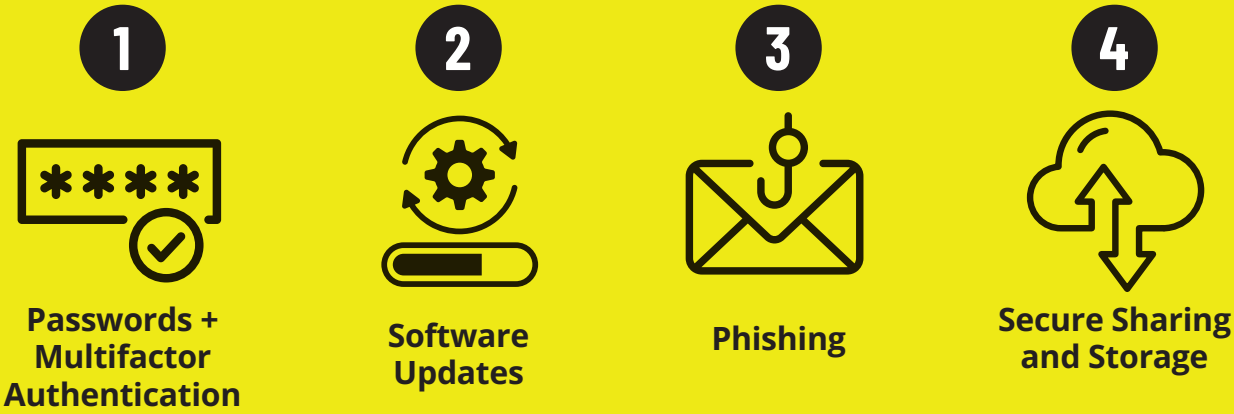
AI is not a single technology, but a broad category of computational methods designed to perform tasks that typically require human intelligence. Some forms of AI have been used in business for decades, while newer capabilities, such as generative AI (GenAI), enable systems to create text, images, and other content. Emerging approaches, including agentic AI, are beginning to introduce systems that can act with greater autonomy. While AI agents offer transformative potential, their autonomy introduces distinct security challenges. For more information on the secure use of AI agents see **Agentic AI Guide**.

This guide focuses on the use of GenAI, which is rapidly increasing in companies of all sizes. While GenAI offers significant benefits, it also introduces new cybersecurity risks for companies and can increase the sophistication of some cyber-attacks. For example, companies have a higher risk of exposing confidential information if employees put data and documents into publicly accessible GenAI tools that are not deployed within an organization-controlled IT environment.

GenAI provides powerful tools to improve efficiency in many areas of your operations. The use of GenAI is not going away; it will accelerate. Organizations must establish appropriate governance and management to ensure GenAI is used safely and securely. Fortunately, there are practical steps that can reduce the risk.

ABOUT THIS GUIDE

This document provides practical guidance for small and medium-sized businesses (SMBs) on how to use GenAI responsibly and securely. It complements the **Cyber Readiness Program** and its focus on the Core Four of cybersecurity:



The guidance in this document will help you to identify the cybersecurity and data exposure risks from using GenAI and put basic governance controls in place to manage those risks.

Useful Basic Definitions

There is a lot being written about the use of AI and GenAI in the workplace. In some cases, terms are incorrectly used interchangeably. For many SMBs, GenAI is most commonly used through applications or services, such as Copilot, Gemini, ChatGPT, or Claude, that are powered by one or more GenAI models. These GenAI tools all use at least one large language model (LLM) to help automate daily tasks like writing, researching, and organizing information.

GenAI Tool & GenAI Model: What's the Difference?

GenAI Model: A model is the underlying machine learning algorithm that has been trained on massive datasets. Think of it as the engine — special skills are needed to work on the engine.

GenAI Tool: A tool (or application) is the consumer-facing software built on top of the model. It wraps the model in a user-friendly interface (UI) and adds practical features. Think of it as the car — anybody can drive the car with a little training.

All GenAI tools are powered by at least one GenAI model, but not all GenAI models are packaged as ready-to-use tools.

Generative AI (GenAI) is the broad category of GenAI tools that create new content, such as text, code, images, music, or videos, by learning patterns from data. GenAI tools are built on one or more GenAI models that are the underlying system trained on data that learns these patterns and generates outputs in response to user inputs. Different types of GenAI models can be designed to generate different kinds of outputs, such as text, images, audio, or video, depending on the data they are trained on. A multimodal GenAI tool uses multiple GenAI models to understand or generate multiple types of data, such as text, images, audio, or video, within a single tool. Most GenAI tools, such as Copilot, Gemini, ChatGPT, and Claude, are multimodal. GenAI tools like Gemini, ChatGPT, and Claude use the same name for both the tool and the underlying model family. In contrast, Copilot is a GenAI tool that is primarily powered by the ChatGPT model family.

All LLMs are GenAI, but not all GenAI are LLMs.
All GPTs are LLMs, but not all LLMs are GPTs.

GenAI Models & LLMs: What's the Difference?

LLMs are a type of GenAI model trained on massive text data that can:

- Understand language
- Generate language
- Answer questions
- Summarize information
- Hold conversations
- Solve problems using text

The term LLM is often used interchangeably with GenAI because they were among the first widely adopted generative AI applications. However, LLMs are only one type of model.

All LLMs are GenAI models, but not all GenAI models are LLMs.

LLMs & GPTs: What's the Difference?

A GPT (Generative Pre-trained Transformer) is a specific type of LLM originally developed by OpenAI. The term is also sometimes used more broadly because GPT models became one of the first widely known uses of GenAI. GPTs are a specific type of LLM that follow a particular design (the "transformer" architecture) and training approach.

To get started you need to understand the difference between public and private GenAI tools.

Public and Private GenAI Tools

Understanding the fundamental differences between public and private GenAI tools is essential for data protection and cybersecurity.

Public GenAI tools are accessible to anyone, typically through a website. They are designed to serve a broad range of users and use cases at scale. Think of them like a public library — open to everyone, with shared resources. Some public tools may use information your organization enters to improve or train the tool, which can result in that information later being reflected in outputs to other users outside your organization. ***Never upload confidential, sensitive, or proprietary information into a public GenAI tool unless the provider explicitly guarantees privacy and you trust their data-handling practices.***

Private GenAI tools operate within an organization-controlled environment or under enterprise data protection and governance boundaries. This enables organizations to ensure that their data remains isolated from public use and is not used to train shared models. They can often be trained or fine-tuned on private data, and access is restricted to approved users only. This is more like a company's internal knowledge vault — secure, tailored, and not open to the public. Most major providers offer private GenAI tools for a subscription fee. There are different levels and they may be called enterprise, business or team models. In the paid subscriptions from the major providers your information is private by default. However, be aware that some models have administrative settings that can be turned on to override the default setting and allow your information to be shared.

Understanding Your GenAI Risks

The first step to reducing your risks to an acceptable level is knowing what the risks are so you can manage them. In this section, we discuss the cybersecurity and data exposure risks based on how most companies are using GenAI tools. We provide you with questions to ask inside your organization and questions to ask with third parties (e.g. vendors, customers, suppliers). We also include some considerations that are specific to cybersecurity risks associated with the use of GenAI.

At the simplest level, the biggest risk of using GenAI is exposing your confidential business information to the public, including competitors. To minimize this risk, you need to make sure everyone in your organization knows two things:

1. **What information is considered confidential by our organization.**
2. **Which GenAI tools are public or are private to our organization (if any).**

GenAI risks are not limited to data exposure. Like other business applications, GenAI tools can create cybersecurity risks if they are not managed properly. Many tools also rely on specialized apps, plug-ins, or connections to business systems, such as customer databases, accounting software, or email platforms. These connections can create new access points if they are not properly secured, so organizations need visibility into what employees are using and whether basic safeguards, such as strong passwords, multi-factor authentication, and software updates, are being followed.

GenAI also creates governance and compliance risks for your workforce and third parties. A common example is “Shadow AI,” where employees use unapproved tools because they are unaware of approved-use policies or find those policies too difficult to follow.

Organizations also need to guard against over-reliance on AI outputs. GenAI tools can help draft, summarize, research, and organize information, but their responses may be inaccurate, incomplete, outdated, or overly confident. This creates risk when employees use AI-generated content for business, legal, financial, customer, or security decisions without checking it. To manage this risk, treat AI as an assistant, not an authority: require human review for important decisions, train employees to verify outputs against trusted sources, and make clear that people remain accountable for what they send, publish, approve, or act on.

GenAI can also make cyberattacks faster, more convincing, and harder to detect. Attackers can use AI to write realistic phishing emails, impersonate trusted people, automate attacks across many organizations at once, and use prompt injection, where malicious instructions hidden in emails, documents, or websites trick GenAI tools into bypassing safeguards, exposing sensitive information, or producing misleading outputs. This makes resilience essential: businesses need the ability to respond quickly, recover from incidents, and continue operating when prevention alone is not enough.

In the following section, we provide questions you can use to help to understand your risks.

Internal Risks

The biggest internal risk is employees inputting sensitive business or customer data into public GenAI tools. However, there are steps you can take to reduce the risk of data exposure.

Use the following questions to assess cybersecurity risks related to to understand the risk from your employees and contractors using GenAI tools:

Top Ten Questions to Ask	Responses / Notes
1 Are there public or private GenAI tools approved for use by your organizations AI policy? If so, which ones?	
2 What GenAI tools are employees actually using today (approved or unapproved)?	
3 Do we have an up-to-date inventory of approved GenAI tools and use cases across the company, including any apps or plug-ins?	
4 What types of company or customer data, if any, have already been shared with public GenAI tools?	
5 Do employees clearly understand what constitutes confidential or customer data when using GenAI tools?	
6 Are clear GenAI usage policies in place and communicated to employees?	
7 Do customer contracts, privacy notices, and policies permit current GenAI use?	
8 Who is accountable for GenAI-related decisions or errors within the organization?	
9 Is there a defined approval process for new GenAI tools or GenAI use cases?	
10 Would employees know how — and feel safe — reporting a GenAI mistake?	

Third-Party Risks

Use the following questions to assess cybersecurity risks related to your vendors, suppliers, and partners to understand the level of risk they pose from using GenAI tools:

Top Ten Questions for Third Parties	Responses / Notes
1 Do you use GenAI in the products or services provided to us?	
2 If so, where and how?	
3 Is our data used in your private GenAI tools?	
4 Is our data used in any public GenAI tools used by your organization?	
5 Do you have a formal policy on the use of GenAI that has been communicated to employees?	
6 How long is our data retained within your GenAI tools and how can the data be deleted?	
7 Do any third parties have access to our data when it is put in your GenAI tools?	
8 What security controls protect data used in your GenAI tools (encryption, access controls, monitoring)?	
9 How do you detect, respond to, and notify customers of GenAI-related incidents or data exposure?	
10 How do you ensure GenAI use complies with applicable laws, regulations, and any contractual requirements?	

Cybersecurity Risks

Use the following questions to assess cybersecurity risks related to the use of GenAI by employees, contractors, and third parties:

Top Five Questions to Assess Cybersecurity Risk	Responses / Notes
1 What is the password policy for accessing GenAI tools?	
2 Is the use of multi-factor authentication required for accessing GenAI tools?	
3 Who is responsible for updating any software related to the use of GenAI?	
4 Are employees and contractors using personal devices to access public or private GenAI tools for work?	
5 Have employees and contractors been trained on the safe use of GenAI in the last 12 months?	

Recommended Actions to Reduce Risk

GenAI tools can transform how you run your business but using them without basic guardrails is risky. Protecting your business doesn't require expensive technology or complex policies — it simply requires a shift in daily habits. By focusing on a simple three-step journey of Awareness, Commitment, and Action, you can confidently harness the power of GenAI while keeping your valuable business data safe.

Build Awareness

- Train employees and contractors on the risks and secure usage of GenAI tools.
- Support the training with short, frequent communications

Gain Commitment

- Send messages from senior people in the organization about the importance of secure GenAI use
- Obtain signed commitments from employees that they understand the GenAI Governance rules and agree to comply

Take Action

- Track which GenAI tools are being used and keep a central inventory of approved tools and approved users
- Verify that humans are checking client- or public-facing GenAI-generated content before release
- Get approval before downloading a new GenAI app or extension
- Take reasonable steps to classify data — at least into public and confidential categories
- Contact your manager if you accidentally paste sensitive data into an unapproved GenAI tool
- Improve prevention by verifying that employees are following CRI's Core Four policies on Passwords + Multifactor Authentication

Sign up for the free **Cyber Readiness Program**.

GenAI Governance Basics

Integrating GenAI into daily workflows can significantly boost productivity, and its use in business will only continue to grow. To minimize exposing your business to unnecessary risks, organizations must establish clear governance, policies, and training.

This section provides a sample GenAI usage policy you can adapt. Legal review is recommended, particularly if your organization collects, stores, and/or processes personally identifiable information (PII) or protected health information (PHI). This document does not provide legal advice.

Use the sample Frequently Asked Questions document (below) to communicate expectations to employees and contractors. Make it widely available in your organization to build awareness of what is allowed and what is not allowed. Having a solid policy is one critical step. Clearly communicating your expectations is what brings the policy to life and reduces your risk.

Sample Policy: Acceptable Use of Generative AI (GenAI)

Effective Date: [Insert date]
Applies to: All employees, contractors, and temporary staff
Owner: [Role or person responsible]
Date Last Updated:

Introduction

This policy outlines how generative artificial intelligence ("GenAI") tools may be used in a safe, responsible way. The goal is to protect data, reduce cybersecurity risks, and ensure GenAI supports — not replaces — human judgment. For this policy, the term GenAI tool also specifically includes large language models (LLMs).

This policy applies to any GenAI tool used for work purposes involving any organization-related data, on any company-issued or personal device.

Our policy clearly differentiates between what you can do using public GenAI tools and private GenAI tools. It is your responsibility to know whether a GenAI tool you plan to use is public or private.

- **Public GenAI Tools:** These tools are accessible to everyone. Any information you enter may be used to train future models, meaning our proprietary data or client secrets could inadvertently be shared with the public. ***Never enter sensitive or confidential data in public GenAI tools.***
- **Private GenAI Tools:** These are secure tools operating under our enterprise data protection and governance boundaries. They offer similar capabilities as public tools but provide a secure space for our data. Information entered here is not used to train public models and stays under our control.

Approved Uses of GenAI Tools

- Use approved private GenAI tools for work-related tasks, including drafting, summarizing, idea generation, and analysis, when those tools are provided or approved by the company.
- Avoid using public GenAI tools where possible to minimize the risk of data exposure. However, if needed, public GenAI tools can be used for general, non-confidential purposes, such as researching concepts, generating high-level ideas, or improving writing clarity.
- All output must be reviewed by a human before use. These tools must be used responsibly, ethically, and in a way that protects organization, client, and personal information.

Use of Company-Approved GenAI Tools

- Only use the public or private GenAI tools approved by our organization for anything related to your job. This applies whether you are using a company-issued device or a personal device.
- Do not create new accounts in any GenAI tool with your work email account without approval.

Prohibited Use of GenAI Tools

- Do not enter confidential, proprietary, personal, or sensitive information into public GenAI tools. This includes client information, internal documents, non-public financial data, personal data, passwords, or security credentials. When in doubt, assume data is sensitive.
- Do not rely on GenAI output as final or authoritative without appropriate human review.
- Do not present GenAI-generated content as verified unless it has been checked for accuracy.
- Do not let AI make the final decision on significant financial, commercial, technical, or personnel matters without human approval.
- Never use GenAI to generate unlawful, harmful, or intentionally misleading content.
- Never use GenAI tools to attempt to bypass the company's security software or access restrictions.

Data Protection and Confidentiality

- Information entered into public GenAI tools can be stored, processed, or reused by third parties. Putting any company information into a public GenAI tool is the same as publicly releasing it.
- Information entered into private GenAI tools must be consistent with existing confidentiality, data protection, and information security policies, just like all other tools. If it is client or supplier information, our use must be in accordance with our contracts with them.

Accountability

- Users are responsible for the appropriate use of GenAI tools and for reviewing, validating, and approving any output before it is shared or acted upon.
- Misuse of GenAI tools may result in corrective action, consistent with company policy.
- GenAI can be wrong. You are responsible for verifying facts, checking sources, and ensuring accuracy and compliance.

Reporting Issues or Concerns

Immediately report accidental data exposure or suspected GenAI-related security incidents.

Violations of This Policy

Violations may result in disciplinary action, loss of access, or legal consequences.

Employee Acknowledgement Form

I acknowledge that I have received, read, and understand the company's Acceptable Use of Generative AI (GenAI) Policy.

I agree to comply with this policy and understand that failure to do so may result in disciplinary action, up to and including termination of employment.

I understand that I am responsible for protecting company, customer, and employee data when using GenAI tools and for reporting any suspected misuse or security incidents.

Employee/Contractor Name: _____

Job Title: _____

Signature: _____

Date: _____

Frequently Asked Questions about Using GenAI

Can I use the public versions of GenAI tools, like ChatGPT, Copilot, Gemini or Claude at work?

When capabilities are similar, we recommend using private GenAI tools to minimize the risk of accidental data exposure. When needed, use of public versions is allowed, but only for general, non-confidential tasks. Never paste sensitive business information or customer data into free public tools. If your organization has an approved Enterprise or Private subscription, you may use those specific versions for tasks involving confidential data, as they keep your information secure.

What counts as confidential information?

Anything not publicly available, including business plans, financial data, customer information, supplier information, and employee information.

What counts as personally identifiable information (PII)?

Any data that can be used to identify, contact, or locate a specific individual, including a name, Social Security number or national ID number, passport number, email address, home address, or phone number.

Can I use GenAI with customer or supplier data?

Only in company-approved private GenAI tools.

Who is responsible for GenAI-generated content?

You are. GenAI assists, but humans remain accountable.

What if I accidentally shared confidential data?

Report it immediately. Prompt reporting helps reduce risk.

How do I know if a GenAI tool is approved?

Check company guidance or ask your manager, IT, or compliance team.

If you would not share it publicly, do not enter it into a public GenAI tool.

CYBER READINESS
INSTITUTE

cyberreadinessinstitute.org