CYBER READINESS
INSTITUTE

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

Reducing Data Exposure & Cybersecurity Risks

FEBRUARY 2026

Introduction

Artificial Intelligence (AI) is reshaping business operations by enabling greater efficiency, improved analytics, and enhanced customer engagement. At the same time, AI 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 systems and algorithms 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.

Newer AI capabilities, like GenAI, introduce new cybersecurity risks for companies and increase the sophistication of cyber-attacks. The use of AI, especially GenAI, is rapidly increasing in companies of all sizes. Companies have a higher risk of exposing confidential information if employees put data and documents into public GenAI tools, like ChatGPT, Gemini or Copilot.

Effective governance is the key for companies to use GenAI effectively and securely.

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 identify the cybersecurity and data exposure risks from using GenAI and put basic governance controls in place to manage those risks.

Useful Basic Definitions

All LLMs are GenAI, but not all GenAI are LLMs.
All GPT models are LLMs, but not all LLMs are GPTs.
(Read this page if you need more detail.)

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 small and medium-sized businesses, Large Language Models (LLMs) are the most frequently used type of GenAI.

GenAI & LLMs: What's the Difference?

GenAI is the broad category of AI that creates new content (text, images, music, code). Large Language Models are a specific type of GenAI focused on understanding and generating human language, trained on massive text datasets. The broader category of GenAI includes tools that generate music, images or computer code. LLMs are specialized tools within the broad GenAI category for generating text. All LLMs are GenAI, but not all GenAI are LLMs.

LLMs & GPTs: What's the Difference?

LLM is the broad category of AI trained on massive text data, while GPT (Generative Pre-trained Transformer) is a specific model of LLMs developed by OpenAI. Think of it like this: all GPT models are LLMs, but not all LLMs are GPTs. Microsoft's Copilot is a GPT because it is built using OpenAI, but Google's Gemini is not because it is built using a proprietary model.

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, and specifically LLMs. 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 LLMs are public and which LLMs are private (if any)**

From a cybersecurity perspective, using GenAI also brings some risks. Many of the LLMs have special purpose applications and plug-ins. It is important for you to have visibility into what apps and plug-ins are being used and if employees are following essential cybersecurity policies in their use (e.g. password length, multi-factor authentication, software updates).

In addition, hackers have been able to create fake websites that look like GenAI tools and LLMs. They are used to obtain confidential information, user names, and even passwords. This highlights the need for using MFA to reduce risk.

To get started you need to understand the difference between public and private Large Language Model.

Public and Private Large Language Models (LLMs)

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

Public LLMs — like ChatGPT, Gemini and Copilot — are accessible to all. They have a huge amount of information, but any information you put into it is accessible to all.

Private LLMs are just for your organization. They provide you with more control over data security, but they lack the enormous amount of publicly available information.

Internal Risks

These are the top ten questions to ask in your organization to understand your risk from your employees and contractors using GenAI.

Top Ten Questions to Ask in Your Organization		Response / Notes
1	What GenAI or LLM tools are employees actually using today (approved or unapproved)?	
2	Do we have an up-to-date inventory of GenAI and LLM tools and use cases across the company, including any apps or plug-ins?	
3	What types of company or customer data have already been entered into public GenAI tools, if any?	
4	Do employees clearly understand what constitutes confidential or customer data when using GenAI tools?	
5	Do we have clear policies on the use of GenAI that have been communicated to our employees?	
6	Do our customer contracts, privacy notices, and policies allow for our current GenAI use?	
7	Who is accountable for GenAI-related decisions, errors, or harm within the organization?	
8	Do we have a defined approval process for new GenAI tools and GenAI use cases?	
9	Where are we relying on GenAI outputs without consistent human review?	
10	If a GenAI-related mistake occurred tomorrow, would employees know how — and feel safe — to report it?	

Third-Party Risks

These are the top ten questions to ask your vendors, suppliers and partners to understand the level of risk they pose to your organization from using GenAI.

Top Ten Questions for Third Parties	Response / Notes
1 Do you use GenAI or LLMs in providing products or services to us?	
2 If so, where and how?	
3 Is our data used in your private LLMs?	
4 Is our data used in any public LLMs used by your organization?	
5 Do you have clear policies on the use of GenAI that have been communicated to your employees?	
6 How long is our data retained within your GenAI systems and how can we request deletion?	
7 Which third parties, sub-processors, or LLM providers are involved in your AI systems?	
8 What security controls protect data used in your GenAI systems (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

These questions are more specific to assess cybersecurity risks related to the use of GenAI by employees, contractors, and third parties.

Top Five Questions to Assess Cybersecurity Risk	Response / 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 accessing public or private GenAI tools for work using personal devices?	
5 Have employees and contractors been trained on the safe use of GenAI in the last 12 months?	

GenAI Governance Basics

GenAI provides your organization with powerful tools to improve efficiency in many areas of your operations. The use of GenAI is not going away — it will accelerate. It is your responsibility to establish the governance and management needed for how GenAI can be used safely and securely. There are practical steps you can take to reduce the risk.

In this section, we provide a sample GenAI usage policy for you to adapt as needed. If necessary, have your policy reviewed by a lawyer to make sure it is aligned with any relevant laws, especially if your organization collects, stores and/or processes Personally Identifiable Information (PII) or Protected Health Information (PHI).

We have also provided a sample Frequently Asked Questions document. Use this to communicate your 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 explains how our organization may use generative artificial intelligence ("GenAI") tools in a safe, responsible way. Our goals are to protect data, reduce cybersecurity risks, and ensure GenAI supports — not replaces — human judgment. For this policy the term GenAI 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 — like ChatGPT, Gemini and Copilot — are accessible to all. They have an immense amount of information, but any information you put into it is accessible to all.

- Private GenAI tools are just for our organization. They provide us with more control over data security, but they lack the enormous amount of publicly available information.

Approved Uses of GenAI Tools

- You may 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.
- You may use public GenAI tools for general, non-confidential purposes, such as learning 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.
- GenAI must not be used to make final decisions, generate unlawful or misleading content, or bypass security controls.

Data Protection and Confidentiality

- Information entered into public GenAI tools can be stored, processed, or reused by third parties. Putting any of our information into public GenAI tools is the same as publicly releasing it.
- Private GenAI tools are designed to provide greater data protection, but all existing confidentiality, data protection, and information security policies still apply.

Accountability

- Users are responsible for the appropriate use of LLMs 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 Acknowledgment 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 public GenAI tools, like ChatGPT, Copilot, or Gemini, at work?

Yes, but only for non-confidential tasks and never with confidential or customer data.

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 name, social security or national ID number, passport number, email address, home address, phone numbers.

Can I use GenAI with customer or supplier data?

Only in company-approved private GenAI tools and only when necessary.

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