NSSF® QUICK GUIDE

PROJECT CYBERSAFE™

Artificial Intelligence

Why should this be on your radar?

Artificial Intelligence (AI) is rapidly transforming how organizations create content, analyze information, do research, and get work done. However, without appropriate guardrails, AI introduces a number of risks including data security, privacy, accuracy, compliance, and ultimately, reputation.

What Can You Do?

1. **Get consensus from leadership on the appetite for AI use.**
   a. Do you want to use AI freely or only in certain controlled cases?
   b. Is it ok to produce work product with AI or only use for time saving repetitive tasks?
   c. Do you treat AI as an employee? (high level of autonomy and trust)
   d. Do you treat AI as an intern? (requires closer supervision and review)

2. **Consider creating a restrictive default overarching AI policy**
   Artificial Intelligence:
   a. AI tools are currently not approved for general use.
   b. An exception list will be maintained by IT and published on the company intranet.
   c. Access to AI tools and features may be requested via the Help Desk and if approved will be added to the exception list.
   d. Company data is considered Confidential Proprietary Business Information and must never be input into an AI system.
   e. Employees are expressly prohibited from using AI (generative or otherwise) to generate work product.

3. **Have a process to evaluate, approve, and record AI tool usage**
   a. Include a process for end users to request an evaluation.
   b. Ensure the process is visible to your end users and they can easily find your list of approved tools.
   c. Ensure your process (including evaluation criteria) is documented and the results of any evaluation are recorded including specific use cases.
   d. Periodically review your decisions and adjust as needed.

4. **Document and share guidance for end users for approved usage and consider training for specific use cases.**

continued →

Additional Considerations

1. **AI Evaluation:**
   a. What is the specific tool and use case?
   b. What data will be used with the tool?
   c. Data Location
      i. Where does the data sit?
      ii. Is the tool a shared resource or is it an instance that lives within your tenant?
      iii. Is it used outside of your tenant for any reason?
      iv. Are there artifacts of the tool that remain? (ex: transcripts)
      v. Can any artifacts be aged off?
   d. What is the cybersecurity footprint of the vendor?
      i. Do they have a good track record?
      ii. Do they have a good overall approach to cybersecurity?
      iii. Have they had any past incidents of concern?
   e. Do you have a contract, NDA, MSA, etc. or is this a prosumer subscription?

2. **AI Usage End User Guidance:**
   a. Is the AI tool on the approved usage list?
   b. Is the intended use case approved?
   c. Is the data used with the tool public or confidential proprietary business information?
   d. Are you using the tool to give insight to a human process or replacing a human process?
   e. Do you have a plan to review the results for accuracy / hallucinations?
   f. Do you need to disclose the use of AI in this process?

Links and Additional Resources

- Fellsway doc on their website?
- For more information on this and other topics, please visit projectcybersafe.com