Generative AI Security Policy

Approval of GenAI Chatbots and/or 3rd Party Applications	To ensure that GenAI tools align with organizational standards and to safeguard against potential risks to security, GenAI tools must be approved, inventoried, and used in a secure manner	☐ Employees must submit Generative AI tool or platform intended for use for approval and review prior to use ☐ The organization will conduct periodic inventories to detect and map all Generative AI tools currently in use, ensuring alignment with approved application lists ☐ Employees are prohibited from using unapproved GenAI tools or platforms for any company- related activities
Integrating GenAI Into a Company Product or Process	Integrating GenAI into the company's products or processes should be done in a manner that ensures that aligns with organizational objectives, respects ethical standards, and adheres to industry best practices	☐ All models utilized to store or transfer data are classified based on the data processed ☐ Access to data models is strictly controlled.The usage of private AI models is monitored for both input and output ☐ Data is anonymized before being input into the data model ☐ Data output is monitored for hallucinations ☐ Use only certified and non-vulnerable open-source models or secured foundation models. ☐ Model training data is vetted or fine-tuned
Creation of GenAI Guidelines	Limit access to authorized personnel, ensuring that only those with proper clearance can leverage GenAI capabilities	☐ Set classification and access control to unauthorized/authorized roles, departments, and classes to GenAI tools ☐ Establish monitoring mechanisms to track interactions with your GenAI policy throughout the lifecycle ☐ Define roles and responsibilities for individuals involved in GenAI development and deployment ☐ Develop mitigation strategies to address identified risks, emphasizing security measures and data protection

Generative AI Security Policy

Safe Usage of Consumer AI Products	Establish a framework that ensures the secure, ethical, and responsible use of GenAI tools within the organization. All usage of consumer AI generators such as ChatGPT, Bard, and Bing Chat within the organization must be handled securely	☐ Prohibit the use of sensitive or private data in input prompts ☐ Employees who generate content with generative AI should follow ethical guidelines ☐ Employees are prohibited from generating content that could be used to commit fraud, crime, impersonation or harm to a person or the company
GenAI Security Awareness Program	Educate employees on best practices, and common dangers while using GenAI tools	☐ Create an awareness program to educate employees about approved GenAI tools, the dangers of unapproved or malicious GenAI tools, and the necessity of adhering to approved tools only ☐ Educate employees on the standards of prompt creation and safe use of generative AI services ☐ Implement a real-time alert system to proactively deter employees from engaging in insecure practices or disclosing sensitive data to GenAI tools
Generated Content Usage	To ensure the reliability and accuracy of content produced by consumer GenAI products, mitigating potential misinformation, and ensuring alignment with the Organization's standards of quality, all content generated undergo a review and validation process to confirm accuracy and appropriateness before distribution or use. This includes text, code, video, or audio	☐ GenAI generated content is proofed before use ☐ GenAI generated content is verified for factual accuracy ☐ GenAI generated content is checked for biases ☐ GenAI generated content is labeled as to its origin