CYBERSECURITY TEMPLATES

Purpose: The purpose of this policy is to establish guidelines and best practices for the responsible and secure use of generative artificial intelligence (AI) at <Company Name>. Generative AI refers to technology that can generate human-like text, images, or other media content using AI algorithms, and is a rapidly developing area of technology with as yet unclear risks and outcomes.

Version	1.0
Prepared By	John Doe - Chief Information Security Officer
Approved By	Mark Haden - Chief Compliance Officer
Last Modified on	10-May-2024
Distribution List	All Employees and Contractors

Exceptions: Any exception to this policy must be approved by the Information Security Team in advance. Please submit the exception request to infosec@<companyname.com>

Instructions

1. Delete this first page of instructions before using your template.
2. Fields marked as "_________" are placeholders for your information.
3. Replace "<Company Name>" with your entity name
4. This template is provided "as is." Please consult your own legal counsel before use.
5. Replace image in the Footer with your company Logo.

Table of Contents

Generative AI Policy

Applications powered by Generative Artificial Intelligence (GenAI), including chatbots (ChatGPT, Google's Gemini, Microsoft Bing) and image generators (DALL-E 2, Midjourney), can be highly effective for learning, generating ideas, content, code, documents, or prototypes; and synthesizing or reviewing data. However, these content-generating tools pose inherent risks related to security, accuracy, and intellectual property. This policy addresses the unique challenges associated with GenAI, providing employees with clear directives for its appropriate use. Its aim is to safeguard the Company's confidential and sensitive information, protect trade secrets, uphold intellectual property rights, maintain workplace culture, reinforce diversity commitments, and preserve the integrity of <Company Name> and our customer's reputation. The nature of these tools involves developing the depth of content by retaining the material (images, data, etc.) submitted to them to enhance that tool's performance over time. This inherently means the material loaded, which could be confidential, is retained in some fashion and could create a risk to <Company Name> confidential Data.

Policy Statement

1. **PURPOSE:**

   The purpose of this policy is to establish guidelines and best practices for the responsible and secure use of generative artificial intelligence (AI) at <Company Name>. Generative AI refers to technology that can generate human-like text, images, or other media content using AI algorithms, and is a rapidly developing area of technology with as yet unclear risks and outcomes.

2. **SCOPE:**

   This policy applies to all <Company Name> employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or others ("Users") who have access to Generative AI tools, related applications, or platforms (collectively "GenAI tools"). It covers the use of Generative AI on company-owned devices, networks, and systems, as well as any other device which may be used to store <Company Name> data or information ("Data"), including personal or third party devices.

3. **POLICY:**

   When utilized with <Company Name> devices and/or Data, GenAI tools may only be used for business purposes approved by the organization. Such purposes may include content generation for marketing, or other legitimate non confidential activities ("Approved Purposes"). GenAI tools must undergo an approval process before they can be used. This approval process will consist of a vendor evaluation, a legal review, a comprehensive assessment of the Gen AI tool itself, including an analysis of the tool's security features, encryption capabilities, and data handling practices, and a dedicated security assessment, to evaluate the overall security posture of the tool. This approval process can be initiated by submitting an evaluation request to the Information Security team.

3.1 Employee Responsibilities

Use of GenAI tools is generally not permitted at <Company Name>. If you require to use Generative AI for work purposes, we ask that you do so transparently, with accountability, and fully in line with the safeguards set out in this policy.

3.1.1 Authorized Use

- Users must utilize GenAI tools and technologies within the boundaries defined by company policies, guidelines, and legal requirements. This involves using GenAI tools and data solely for Approved Purposes, adhering to company acceptable use policy, and with respect to privacy, security, and ethical considerations.
- Unauthorized use of copyrighted material or infringement of intellectual property rights is prohibited.

- Users must not integrate any GenAI tool with internal company software without first receiving specific written permission from the IT Security team.

3.1.2 Data Privacy

- Users must consider the confidentiality, integrity, and availability to unauthorized third parties of data generated or processed using Generative AI.
- Personal or sensitive information should not be used as input data (“Prompt”).
- Users must exercise discretion when sharing/uploading company information with GenAI tools such as entering Prompts or uploading company documents to GenAI tools.
- Users must not upload or share any data related to customers, employees, or vendors that is confidential, proprietary, or protected by regulation without prior authorization from the IT Security team.
- Users are responsible for ensuring the accuracy, appropriateness, and confidentiality of any information shared.
- Users should avoid generating content that is misleading, deceptive, offensive, or harmful.
- Content generated using Generative AI should not promote discrimination, harassment, violence, or illegal activities.

3.2 Limitations of GenAI tools

While GenAI tools have revolutionized various aspects of technology and decision-making processes, it is important for Users to be aware of their limitations. These limitations include:

- **Bias:** GenAI models are trained on data that may contain biases, which can inadvertently be reflected in the generated outputs. It is crucial to exercise caution and conduct thorough testing to ensure fairness and avoid perpetuating biases in the AI-generated content.
- **Inaccuracy:** GenAI models are not infallible and can produce inaccurate results. The outputs generated by these tools should be carefully reviewed and validated to ensure their reliability and correctness.
- **Lack of Contextual Understanding:** GenAI models often lack the ability to understand context comprehensively. They may struggle with nuances, sarcasm, or ambiguous language, leading to potential misinterpretations or inappropriate responses.
- **Ethical Considerations:** GenAI modeling tools can raise ethical concerns, especially when dealing with sensitive data or generating content that may have legal implications. Users must be mindful of ethical considerations and ensure compliance with relevant laws and regulations. This includes respecting intellectual property rights, not using GenAI platforms to infringe on others' content or proprietary information and complying with licensing and usage restrictions.
- **Limited Generalization:** GenAI models are trained on specific datasets, which means they may not handle situations or data outside of their training domain. It is important to assess the suitability and limitations of the AI model for a given task or problem.

3.3 Attribution

When utilizing GenAI tools, Users must adhere to guidelines for appropriate collaboration and attribution. This includes giving proper credit to content generated by the tools and obtaining necessary permissions for external resources.

3.4 Reporting and Responsible Disclosure

Malicious GenAI tools such as chatbots can be designed to steal or convince you to divulge information. Users shall promptly report any potential ethical or security concerns arising from the use of GenAI tools. Concerns can be reported to their manager or the Information Security team. Responsible disclosure of vulnerabilities, issues, or unintended consequences discovered while using GenAI tools is expected.

4. EXCEPTIONS:

Any exception to this policy must be approved by the Information Security Team in advance. Please submit the exception request to infosec@company.com

5. HOW IS COMPLIANCE WITH THIS POLICY MONITORED?

Compliance Measurement: The Information Security Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, spot checks, internal or external audits, and feedback to the policy owner.

Non-Compliance: Employees and contractors employed by <Company Name> found to have violated this policy will be subject to disciplinary action based on the nature of the violation up to and including termination of employment. Third Parties that are found to have violated this policy will be subject to disciplinary action based on the nature of the violation including but not limited to loss of network and computing access, and other actions the <Company Name> Information security team deems appropriate.

Related Documents	
• Acceptable Use Policy	Link to the sharepoint
• Record Retention Policy	Link to the sharepoint
• Inventory Management Template	Link to the sharepoint

Related Standards or Controls:	
• **NIST CSF SP.PM-29, SP.RA-5**	• PM-29: Outlines the requirements for managing risks associated with AI systems sourced from third-party vendors. • RA-5: Requirements for continuous monitoring and scanning of AI systems for vulnerabilities.

Version History

Version	Date	Description	Author
V1.0	20-Jan-2024	Initial version for review by CIO	CISO

Appendix: Glossary

Asset	Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). Source: Asset(s) - Glossary | CSRC (nist.gov)
Asset inventory	An asset inventory is a register, repository or comprehensive list of an enterprise's assets and specific information about those assets. Source: Asset Inventory | FTA (dot.gov)
Asset owner	The department, business unit, or individual responsible for an IT asset.
Cloud environment	A virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
IT assets	Assets with the potential to store or process data. For the purpose of this document, IT assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers in virtual, cloud-based, and physical environments. Source: CIS Controls v8
End-user devices	Information technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones, and tablets as well as desktops and workstations. For the purpose of this document, end-user devices are a subset of IT assets. Source: CIS Controls v8
IT asset identifier	Often a sticker or tag with a unique number or alphanumeric string that can be tracked within an IT asset inventory. Source: CIS
Mobile end-user devices	Small, enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. Mobile end-user devices are a subset of portable end-user devices, including laptops, which may require external hardware for connectivity. For the purpose of this document, mobile end-user devices are a subset of end-user devices. Source: CIS Controls v8
Network devices	Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of IT assets. Source: CIS Controls v8
Non-computing/Internet	Devices embedded with sensors, software, and other technologies for the purpose of connecting, storing, and exchanging data with other devices and systems over the internet. While these devices are not

of Things (IoT) devices	used for computational processes, they support an enterprise's ability to conduct business processes. Examples of these devices include printers, smart screens, physical security sensors, industrial control systems, and information technology sensors. For the purpose of this document, non-computing/IoT devices are a subset of IT assets. Source: CIS Controls v8
Physical environment	Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network. Source: CIS Controls v8
Portable end-user devices	Transportable, end-user devices that have the capability to wirelessly connect to a network. For the purpose of this document, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of IT assets. Source: CIS Controls v8
Remote devices	Any IT asset capable of connecting to a network remotely, usually from the public internet. This can include IT assets such as end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers. Source: CIS Controls v8
Servers	A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers. Source: CIS Controls v8
User	Employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an IT asset. Source: CIS
Virtual environment	Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work. Source: CIS Controls v8