****

**Artificial Intelligence Security Policy Template**

*By Paul Kirvan, FBCI, CISA*

|  |
| --- |
| **Title:** Artificial Intelligence Security Policy |
| **Department:**  | **Version:** Original |
| **Approved by:**  | **Approval Date:**  |
| **Senior Management Approval:**  |
| **Effective Date:**  | **Last Updated:**  |
| **Author:**  |
| **Scope**This policy applies to the <location of <company name>>.<enter address> |
| **Authority**This policy is hereby approved and authorized.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name Title Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name Title Date |
| **Purpose**The purpose of this policy is to define the activities associated with the provision of cybersecurity for the identification of and response to unauthorized attacks generated either directly or indirectly from the use of artificial intelligence, or AI, systems and technologies. Generative AI (GenAI) is an example of the technology addressed by this policy. These may include, but are not limited to, phishing and ransomware attacks on the organization's information systems, networks, data, databases and other information assets. Additional policies governing other cybersecurity activities will be addressed separately. |
| **Scope**The scope of this AI security policy is all information technology systems, software, databases, applications and network resources that are implemented in on-premises, cloud-based and/or managed service infrastructures needed by the Company to conduct its business. |
| **Statement of Compliance**This policy is designed to be compliant with the following standards: * ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection -- Information security management systems -- Requirements.
* NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations.
* NIST Framework for Improving Critical Infrastructure Cybersecurity.
* FFIEC Information Technology Examination Handbook for Information Security (2016).

From an AI perspective, this policy is developed with guidance from the following standards and frameworks:* ISO/IEC 22989:2022 Information technology -- Artificial intelligence -- Artificial intelligence concepts and terminology.
* ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).
* ISO/IEC 23894:2023 Information technology -- Artificial intelligence -- Guidance on risk management.
* ISO/IEC DIS 27090 Cybersecurity -- Artificial Intelligence -- Guidance for addressing security threats to artificial intelligence systems (currently in development).
* ISO/IEC 42001:2023 Information technology -- Artificial intelligence -- Management system.
* NIST AI Risk Management Framework.
* NIST AI 100-2e2025 "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations."

Cybersecurity policy compliance is managed by the IT data security team, with support from other IT departments. To achieve compliance, cybersecurity processes must include appropriate procedures and identify staffing and technology resources to meet compliance requirements. Cybersecurity vendors and service providers are required to demonstrate compliance with this policy. Compliance verification is performed monthly by the IT department, internal audit or other appropriate entity. |
| **Policy**As part of its duty of care to its customers and as a matter of good business practice, the confidentiality, integrity and availability of all IT applications, data, systems and network resources at <company name> are to be managed by a formal cybersecurity management program. This program will provide a controlled and orderly method by which unauthorized access to <company name> information systems and resources that use artificial intelligence (AI), machine learning (ML) or similar technologies is identified, prevented, captured, analyzed and mitigated, and changes to cybersecurity systems and procedures are requested, tested, approved and communicated for audit and record-keeping purposes.The increasing use of artificial intelligence systems and technology by the company may unknowingly provide opportunities for unauthorized attempts to access <company name> systems and resources. This policy will include references, where applicable, that address security measures potentially impacted by AI technology.1. This policy addresses all <company name> technology, systems, data and networks using artificial intelligence, machine learning or similar technologies implemented in company-owned and managed IT operations facilities; private, hybrid and/or public cloud infrastructures; and all other <company name> IT assets implemented in managed services as identified by IT department management.
2. The IT department will define cybersecurity processes and procedures; secure and utilize specialized software and systems to reduce the threat of cybersecurity breaches associated with artificial intelligence; regularly test the security of the company's perimeters and the cybersecurity vendor's services using penetration tests and other forensic methods; and document all cybersecurity procedures and controls.
3. The above processes and procedures will be designed to address AI-based security events, as well as non-AI events.
4. The IT department will define cybersecurity protocols for identifying, analyzing, managing and eliminating unauthorized security activities that it suspects have been generated through the use of AI technology.
5. The IT department will develop such protocols with guidance from AI-focused standards and frameworks, including ISO/IEC 22989:2022 Information technology -- Artificial intelligence -- Artificial intelligence concepts and terminology; ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML); ISO/IEC 23984:2023 Information technology -- Artificial intelligence -- Guidance on risk management; ISO/IEC DIS 27090 Cybersecurity -- Artificial Intelligence -- Guidance for addressing security threats to artificial intelligence systems; ISO/IEC 42001:2023 Information technology -- Artificial intelligence -- Management system; NIST AI Risk Management Framework; and NIST AI 100-2e2025 "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations."
6. The IT department will prepare and document IT information security and cybersecurity plans; facilitate the maintenance and review of those plans; and ensure that procedures for analyzing potential AI-based attacks are included in these plans.
7. The IT department will periodically conduct risk assessments of the internal and external threats and vulnerabilities of the IT environment, as applicable to all operating IT environments and with an emphasis on the impact of artificial intelligence.
8. To ensure that AI-based events are considered in risk assessments, guidance will be obtained from ISO/IEC 23984:2023 Information technology -- Artificial intelligence -- Guidance on risk management; ISO/IEC 42001:2023 Information technology -- Artificial intelligence -- Management system; and NIST AI Risk Management Framework.
9. The IT department will ensure malware -- e.g., viruses, spam, phishing attacks, ransomware attacks, denial-of-service attacks and other unauthorized access attempts, both non-AI and AI-based -- are prevented through the use of antivirus software and other appropriate cybersecurity prevention and detection resources. It will ensure that cybersecurity and other IT vendors have similar antimalware and AI analysis capabilities and that the use of those services shall be approved by <company name>.
10. The IT department will review available cybersecurity systems -- including systems currently in use -- to determine if they are capable of detecting, analyzing and mitigating AI-based threat signatures and other code that might indicate an AI-based anomaly.
11. In coordination with this cybersecurity policy, the IT department will establish a network perimeter security policy to ensure unauthorized attempts to penetrate the <company name> network perimeter are prevented.
12. The network security policy will include guidance from the reference documents in this policy so that AI-related information is included in the network security policy.
13. The IT department will establish and document a formal process for identifying a possible breach in the network perimeter -- e.g., denial-of-service attack, ransomware attack, phishing -- assessing the breach, determining the nature and possible impact of the breach, notifying <company name> management of the breach, minimizing the impact of the breach as quickly as possible, and documenting the steps taken when dealing with the incident. This process will apply to all operating environments, i.e., company IT facilities and managed services, including cloud environments, whether internal, hybrid and/or public clouds, and will also provide guidance for determining if the attack has AI characteristics.
14. The IT department will establish and document a formal process for identifying a possible internal cybersecurity breach -- e.g., theft of information, social engineering, unauthorized access to systems -- assessing the breach, determining the nature and possible impact of the breach, notifying <company name> management of the breach, minimizing the impact of the breach as quickly as possible, and documenting the steps taken when dealing with the incident.
15. The internal security policy will include guidance from the reference documents in this policy so that AI-related information is included in the policy for identifying internal and external cyberattacks.
16. The IT department will include business continuity and disaster recovery among its cybersecurity controls.
17. The IT department will include incident response management among its cybersecurity controls and will include guidance on how to identify possible AI-based attacks.
18. The IT department will define consequences of AI cybersecurity policy violations.
19. The IT department will define how cybersecurity incidents -- both non-AI and AI-based -- are reported and managed.
20. The IT department, in collaboration with the <company name> legal department, shall prepare and have executed the appropriate service-level agreements with cybersecurity equipment and service providers to ensure acceptable third-party vendor performance and support for AI-based events.
21. Data in use at <company name>, whether at rest or in motion, must be encrypted.
22. <Company name> employees must sign an employee contract agreeing to accept and comply with cybersecurity policies at the time they are hired and on a regular basis -- e.g., annually -- through the employee handbook and/or in contract renewals to account for policy changes over time.
23. All proposed changes to cybersecurity operations, including those activities associated with managing AI-based cybersecurity attacks, are to be documented in detail.
24. Cybersecurity breaches that may impact <company name> IT operations are identified in the information security management system and associated plans, which have been updated to address AI-based attacks.
25. The IT department will develop a schedule of all cybersecurity activities for the company and will ensure these activities are completed on time.
26. The IT department will ensure all cybersecurity policies and associated procedures comply with appropriate legislative, regulatory and contractual requirements, as well as accepted standards and good practice, including the AI standards and frameworks noted in this policy.
27. The IT department will establish and schedule awareness trainings and messages to educate and inform employees about cyberattacks, attacks based on AI, how to identify and report suspicious activity, and how to prevent cyberattacks from occurring, whether working in the office or at home.
28. The IT department will establish a program of regular testing of its cybersecurity systems, incident response and cybersecurity plans, and activities associated with AI attack prevention and detection.
29. All proposed changes to this Artificial Intelligence Security Policy are to be processed and documented by the IT change management system.
 |
| **Policy Leadership****<Title of executive>** is designated as the corporate owner responsible for cybersecurity activities for the Company. Resolution of issues in the support of cybersecurity activities should first be coordinated with IT management, the corporate information security team and others as needed. |
| **Policy Responsibilities*** Policy Approval. The **<title of executive>** is responsible for approving this policy.
* Policy Implementation. The <name of department or individual> is responsible for planning, organizing and implementing all activities that fulfill this policy.
* Policy Maintenance and Updating. The <name of department or individual> is responsible for all activities associated with maintaining and updating this policy.
* Policy Monitoring and Review. The <name of department or individual> is responsible for monitoring and reviewing this policy.
* Policy Improvement. The <name of department or individual> is responsible for defining and implementing activities that will improve this policy.
* Policy Auditing. The <company name> internal audit department, or an approved external audit organization, organizes and coordinates the completion of cybersecurity policy audits, in collaboration with the IT department.
 |
| **Management Review**<Name of department or individual> will review and update this artificial intelligence cybersecurity policy on an annual basis. As changes to this cybersecurity policy are indicated in the course of business, <name of department or individual> may initiate a change management process to update this policy. |
| **Policy Enforcement**The **<title of executive>** will enforce this policy. |
| **Penalties for Noncompliance**In situations where cybersecurity response and recovery activities do not comply with this policy, the IT security team will prepare a report stating the reason(s) for noncompliance and present it to IT management for resolution. Failure to comply with this cybersecurity policy and any service-level agreements established with external cybersecurity firms within the allotted time for resolution may result in verbal reprimands, notes in personnel files and termination for internal incidents, as well as fines, legal actions and such other remedies as deemed appropriate for external incidents. |
| **Policy Location**The policy will be signed, scanned into an electronic file and posted in the following location on the network: <location of policy>. |