Group Assignment 1: Developing a Security Policy for AI Enterprise Applications

Deliverable 3: Executive Summary

Group Members:

Kaydeen Walker ID# 1902433

Alanzo Harris ID#2210195

Iyana Taylor ID#2209566

Lamar Eastman ID#2210172

Module Name: Computer Security

Module Code: CIT4020

University of Technology, Jamaica

Faculty of Engineering and Computing

School of Computing and Information Technology

Tutor: Kevin Johnson

Due: October 6, 2025

Executive Summary

This AI Security Policy sets out the organization's approach to ensuring for safe, ethical, and compliant use of artificial intelligence(AI) in enterprise operations. AI technologies enhance efficiency, streamline decision-making, and drive innovation, but they also introduce risks that must be observed carefully. This policy provides a framework to safeguard sensitive data, protect systems from misuse, maintain compliance with laws and standards, and preserve trust in AI-driven processes.

Key Risks and Challenges

The use of AI brings six major security concerns:

- **Data Privacy:** Exposure of sensitive or personally identifiable information through large-scale data processing.
- **Access Control:** Weak identity management can enable unauthorized access to systems and data.
- **Model Integrity:** AI models can produce biased or inaccurate results if training data is compromised.
- **Threats:** AI-specific risks, such as adversarial attacks, data poisoning, and prompt injections, extend beyond traditional cybersecurity.
- **Compliance:** Misuse of AI could result in breaches of Jamaica's Data Protection Act, GDPR, and other regulatory standards.
- **Ethics:** Lack of transparency and accountability in AI use can perpetuate bias and erode stakeholder trust.

To address these risks, the policy requires proper classification of incidents, monitoring of AI outputs to ensure fairness, allowing different levels of restricted access controls, and following ethical guidelines

Implementation and Accountability

Roles and responsibilities are defined to ensure accountability:

- **Leadership** promotes ethical adoption and ensures regulatory alignment.
- **IT and Security Teams** oversee system integrity, manage threats, and lead incident response.
- **Compliance Officers** enforce adherence to legal and industry requirements.
- **Employees** must complete training and apply AI responsibly.

Conclusion

This AI Security Policy enables the organization to maximize the benefits of AI while minimizing associated security risks. By embedding strong security measures amongst employees, regulatory compliance, and ethical safeguards into AI usage, this ensures the company can push forward with innovative milestones and stay ahead of the competition without setbacks.

Group Assignment 1: Developing a Security Policy for AI Enterprise Applications

Deliverable 1: Written AI Security Policy Document

Group Members:

Kaydeen Walker ID# 1902433

Alanzo Harris ID#2210195

Iyana Taylor ID#2209566

Lamar Eastman ID#2210172

Module Name: Computer Security

Module Code: CIT4020

University of Technology, Jamaica

Faculty of Engineering and Computing

School of Computing and Information Technology

Tutor: Kevin Johnson

Due: October 6, 2025

Table of Contents

Introduction & Purpose

Artificial intelligence represents a transformative advancement in technology that has dramatically improved efficiency and productivity across multiple sectors, including education, healthcare, and particularly the corporate world. In educational settings, AI tools facilitate personalized learning experiences and enhance administrative efficiency. In the medical field, AI algorithms assist in diagnosing diseases and optimizing treatment plans, thereby improving patient outcomes.

Within the corporate sector, AI streamlines operations, enhances decision-making processes, and drives innovation by analyzing vast amounts of data in real time. Despite these remarkable benefits, the rapid advancement of AI technology also introduces significant security risks and ethical concerns. To mitigate these challenges, it is crucial to establish comprehensive policies and regulatory frameworks that govern the development and implementation of AI. By doing so, we can ensure that the technology is used responsibly, protecting sensitive information and maintaining public trust in AI applications.

This policy aims to:

- Protect organizational data, systems, and users from AI-related risks.

- Ensure compliance with applicable laws and industry standards.

- Guide employees and contractors in the ethical use of AI tools.

- Promote accountability and transparency in AI usage.

Scope:

This policy applies to:

- All employees, contractors, and third-party partners using AI technologies for the organization.

- All AI systems, applications, and services, whether developed in-house or by external vendors.

- Data and resources used in training and interacting with AI systems.

This ensures all AI interactions meet high standards of security, ethics, and compliance.

Risk Analysis of AI Adoption

Data Privacy Risks

Artificial Intelligence (AI) typically relies on large-scale data collection and processing to fulfil user requests. Though this data is collected from various sources, including user interactions, record and file attachments, and sensor input, crucial data privacy concerns are still being raised regarding consent (what data may be collected, if any at all) and transparency (how that data is being used) (Chukwunweike et al., 2024). Furthermore, AI systems may aggregate the data collected from these many sources to create detailed profiles of individuals and organizations. While this may enhance user experience, the risk of invasive profiling and surveillance increases significantly (Ijaiya, 2024), as these parties may be unaware of this process and who their profiles are being sold to. And with that, managing data input rules and anonymization is crucial, especially for corporations.

Access Control Issues

Access Control Issues, in the context of AI and Large Language Model (LLM) adoption, relates to how identity, authentication, and authorization are implemented and govered — be it on a network, system, or in an organization, et cetera — especially considering the unique technical and social threats posed by these computing technologies. There is a lack of standardization regarding access control, entitlement, and governance in AI systems (Alomari et al., 2021), and according to Polemi, 2024, the absence of proper frameworks can lead to challenges in holding AI systems accountable for decisions. Recall the risk of data analytics and invasive user profiling by these sophisticated algorithms discussed in the "Data Privacy Risks" section, unauthorized access to these details can result in privacy breaches and compromise companies' autonomy. Therefore, enforcing role-based access controls reduces exposure of critical company data.

Model Integrity

Ensuring that the foundational principles of company/ enterprise processes, be it cybersecurity, compliance, or privacy, are maintained when AI tools are integrated is what Model Integrity is fundamentally about. Doskaliuk, 2025, explains that the quality of AI and LLM's outputs is directly influenced by the data they have been trained on/ exposed to, and if these datasets contain inherent biases (those related to gender, race, geographic location, or publication trends, et cetera), AI may perpetuate them in suggestions or assessments. This poses a risk to the objectivity and fairness of business processes and could erode trust in company systems. Therefore, regular monitoring and auditing will be required to effectively manage bias and preserve the integrity of the AI and LLMs adopted.

Threat Mitigation

Threat Mitigation refers to the strategies and solutions developed to safeguard systems against various security threats and challenges, with the primary goal being to ensure safe, robust and ethical deployment of company data and applications. Threat Mitigation, as it relates to AI adoption, focuses on protecting systems from anything that may compromise their functionality and reliability (Yazmyradov, 2024). Securing AI and LLMs is a crucial security concern due to technical vulnerabilities and ethical implications, and key threats (including adversarial attacks, data poisoning, and model inversion, et cetera) can severely compromise the core security pillars — Confidentiality, Integrity and Availability (Yazmyradov, 2024). With that, the company must adapt its threat mitigation models to AI contexts since traditional security measures don't address AI-specific risks in full.

Compliance Risks

Compliance, which is an organization's adherence to laws, regulations, standards, internal and external policies, continues to struggle due to the increasing complexity of regulatory environments and growing business data, which often relies on resource-intensive, human-error-prone, manual processes. AI systems must adhere to strict data protection laws in relation to compliance, like the General Data Protection Regulation (by the European Union, EU) or Jamaica's Data Protection Act (Aror & Mupa, 2025; Stewart, 2025; Clement 2025); the risk of AI misuse in handling sensitive data could lead to significant breaches or unauthorized access, resulting in severe legal and financial consequences (Aror & Mupa, 2025; Clement 2025). Strong compliance rules ensure lawful use of AI in company operations, and businesses must ensure that AI tools do not violate privacy laws or expose confidential information.

Ethical Concerns

Adopting AI in business comes with ethical implications stemming from significant societal, operational, and legal risks that need to be addressed before, during, and after business operations. One such ethical implication is the perpetuation of societal inequality; algorithmic bias (discussed in the “Model Integrity” section) is one of the most pressing ethical concerns of AI adoption as systems reproduce social prejudices received from their training data (Ghosh, 2025; Ahmed, 2025). Destruction of trust and reputational harm is another ethical implication which relates to the degree to which AI systems and their decision-making logic are understandable to users. Ahmed (2025) states frankly that the issue is with the lack of transparency of many AI models, making it difficult to understand and explain how they arrive at specific conclusions, and without clarity, users lack the power to challenge or verify output, making the system(s) less trustworthy and harder to hold accountable. As such, embedding ethical guidelines protects the interests of the company and its clients.

Policy Statements & Security Controls

1. Data Privacy & Protection

- Policy Statement: Employees must safeguard the confidentiality, integrity and availability of company and client data when using AI systems. Sensitive, confidential or personally identifiable information (PII) must not be uploaded, shared or stored in external AI platforms without explicit approval from the Information Security Team.
- Controls:
    - Classify data into categories (e.g., public, internal, confidential, restricted).

    - Prohibit sharing of restricted or confidential data (e.g., financial records, employee PII, client contracts) with external AI tools.
    - Use anonymization and encryption when processing sensitive datasets internally with AI applications.
    - Maintain audit logs of all AI data interactions.

2. Access Control & Authentication

- Policy Statement: Access to AI systems must be strictly controlled to authorized personnel based on business needs.
- Controls:
    - Implement role-based access control (RBAC) to limit use of AI tools to approved users.
    - Enforce multi-factor authentication (MFA) for access to enterprise AI applications.
    - Regularly review and update access privileges (quarterly or upon employee role change/exit).
    - Prohibit the use of personal accounts for enterprise AI-related tasks.

3. Model Usage & Integrity

- Policy Statement: AI applications must be used responsibly, ensuring accuracy, reliability and alignment with company goals. Outputs must always be validated before use in decision-making.
- Controls:

  - Define acceptable use cases (e.g. drafting documents, analyzing reports, generating code).
  - Prohibit misuse (e.g., generating discriminatory content, misinformation or malicious code).
  - Require human review and approval of all critical outputs (e.g. client communications, financial analysis).
  - Conduct periodic model testing and validation to detect bias, errors or drift.

4. Threat Detection & Mitigation

- Policy Statement: The organization will actively monitor and respond to AI-related security threats, ensuring resilience against adversarial attacks and misuse.
- Controls:
  - Deploy monitoring tools to detect abnormal AI usage patterns (e.g. data exfiltration, prompt injection attacks).
  - Establish incident response protocols for AI-related breaches or misuse.
  - Conduct regular penetration tests and red-team exercises on AI applications.
  - Provide employee training on identifying and reporting suspicious AI outputs or threats.

5. Compliance & Regulations

- Policy Statement: All AI adoption and usage must comply with applicable legal, regulatory and contractual requirements.
- Controls:

    - Align with local data protection laws (e.g. Jamaica Data Protection Act) and international standards (e.g. GDPR, ISO/IEC 27001).
    - Maintain documentation of AI system audits and compliance reviews.
    - Require third-party AI vendors to meet company security and compliance requirements.
    - Review compliance obligations annually and update the policy accordingly.

6. Ethical Usage Guidelines

- Policy Statement: AI must be used ethically, promoting fairness, accountability and transparency in all operations.
- Controls:
    - Prohibit discriminatory or biased outputs from being used in decision-making.
    - Require clear disclosure when AI-generated content is used in external communication.
    - Promote explainability and transparency of AI-driven decisions, especially in HR, finance or customer service.
    - Establish an AI Ethics Committee to review high-risk use cases.

Implementation & Training

To ensure effective and safe adoption of AI enterprise applications, the organisation will implement the following roles and responsibilities.

1. **Roles & Responsibilities**
    - **Executive Leadership and Management**

    - Ensure and oversee the adoption of AI strategies, legal requirements and regulatory frameworks (eg, Jamaica Data Protection Act, GDPR).
    - Promote an ethical and secure culture of AI usage within the organisation
- **Information Technology Staff**
    - Deploy, modify and maintain AI systems and infrastructure related to such
    - Provide technical support to staff.
    - Apply security patches, updates, and vulnerability management procedures for AI tools
    - Provides Technical Support to staff regarding AI usage.
- **Security Team**
    - Conduct risk assessment of AI-related threats (eg, prompt injection, adversarial inputs and model poisoning)
    - Monitor AI systems for signs of breaches, misuse or data leakage.
    - Lead Incident response procedures, including containment, recovery and post-incident analysis.
- **Data Protection & Compliance Officer**
    - Ensure AI usage adheres to local and international data protection policies
    - Approve guidelines on the classification and handling of sensitive data.
    - Conducts compliance audits to evaluate adherence to regulatory and ethical standards
- **Employees**
    - Conduct the usage of AI tools responsibly in accordance with the organisation's policies.

    - Avoid entering and uploading sensitive or confidential data on the organisation or its clients into public AI platforms.
    - Fully complete all mandatory AI usage and security awareness training procedures before being granted access to AI systems and tools

2. Training Requirements

The Organisation will establish a comprehensive training program to ensure all stakeholders are adequately trained and prepared to use AI tools to their full extent securely and responsibly.

- **General Staff Training**
    - Data Safety Practices: Employees must not input confidential company or client data, concerning financial records or personal information, into external AI tools
    - Risk Awareness: Covers common AI-related threats, such as bias, misinformation and prompt injection attacks
    - Policy Awareness: Staff must be familiar with what constitutes acceptable and unacceptable AI usage within the company.
    - Reporting Procedures: training will emphasise how and to whom to report in case of an incident.
- **Specialised training (IT & Security Team)**
    - Threat Response and Mitigation: Practical Exercise on Adversarial Attacks, model exploitation, and system hardening.
    - System Auditing: Techniques for monitoring AI logs, anomaly detection, and access control enforcement.

    - Incident Response: Training in simulation exercises for AI-related breach scenarios

- **Management and Leadership Training**
    - Regulatory Compliance: Training in the obligations of leadership under GDRP, the Jamaica Data Protection Act (JDPA).
    - Ethical AI usage: Modules covering bias detection, fairness, accountability and transparency in AI decision-making.
- **Frequency and Delivery**
    - Annual Refresher Course: Organisation-wide update on emerging threats, regulatory changes and new safeguards.
    - Awareness Campaigns: Ongoing reinforcement through internal communications and reminders on AI safety practices.

Incident Response & Reporting

Detecting the problem

“Monitoring and logging mechanisms should be in place to detect anomalous behaviour, data drift, or security breaches in AI systems. Incident data should be recorded to support investigations and post-incident analysis. (National Institute of Standards and Technology [NIST], 2023)

Employees must have their systems monitored to keep track of any form of malicious practice or misuses.

Immediate report to the IT Security Team

Incidents that have appeared are to be reported to superior IT specialist immediately

Contain and investigate the issue

“Organizations should provide training to staff and contractors on how to recognize and report AI-related incidents, including potential harms, ethical violations, or security breaches.” (NIST.Ai….)

The incident must be contained ,the system must be backup in case memory alteration or potential deletion

Notify leadership, legal, and regulators if needed.

“Incident response plans should define escalation procedures and communication channels for notifying relevant stakeholders, including senior management and regulatory bodies when appropriate.”

Review the incident afterwards to prevent it happening again.

“Organizations should maintain processes for continuous improvement of their AI governance, including incorporating lessons learned from incidents.”

Policy Review & Updates

Frequency of Review (regular review of the AI policy)

“AI risk management policies and procedures should be reviewed periodically and updated as AI technologies, risks, and regulations evolve.”

Responsible Parties

“Reviews should involve multidisciplinary stakeholders and incorporate lessons learned from incidents and changes in the operating environment.”

Continuous training to stay consistent and attentive

“Organizations should maintain processes for continuous improvement of their AI governance, including incorporating lessons learned from incidents.”

Monitoring for Changes

“Regular assessments of compliance with applicable laws, standards, and ethical guidelines” and “updated as AI technologies, risks, and regulations evolve.”

References

Ahmed, I. (2025). Navigating Ethics And Risk In Artificial Intelligence Applications Within Information Technology: A Systematic Review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 579-601. https://doi.org/10.63125/590d7098

Alomari, M. K., Khan, H. U., Khan, S., Al-Maadid, A. A., Abu-Shawish, Z. K., & Hammami, H. (2021). Systematic Analysis of Artificial Intelligence‐Based Platforms for Identifying Governance and Access Control. *Security and Communication Networks*, *2021*(1), 8686469. https://doi.org/10.1155/2021/8686469

Aror, T. A., & Mupa, M. N. (2025). Risk and compliance paper what role does Artificial Intelligence (AI) play in enhancing risk management practices in corporations. *World Journal of Advanced Research and Reviews*, *27*(1), 1072-1080. https://doi.org/10.30574/wjarr.2025.27.1.2607

Chukwunweike, J. N., Yussuf, M., Okusi, O., & Oluwatobi, T. (2024). The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions. *World Journal of Advanced Research and Reviews*, *23*(2), 2550. https://doi.org/10.30574/wjarr.2024.23.2.2550

Clement, M. (2025). Key Compliance Challenges and the Role of AI. https://www.researchgate.net/profile/Mateo-Clement/publication/390919180_Key_Compliance_Challenges_and_the_Role_of_AI/links/680242a1ded43315572ac03a/Key-Compliance-Challenges-and-the-Role-of-AI.pdf

Doskaliuk, B., Zimba, O., Yessirkepov, M., Klishch, I., & Yatsyshyn, R. (2025). Artificial intelligence in peer review: enhancing efficiency while preserving integrity. *Journal of Korean medical science*, *40*(7). https://doi.org/10.3346/jkms.2025.40.e92

European Union Agency for Cybersecurity (ENISA). (2021). Securing Machine Learning Algorithms. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Securing%20Machine%20Learning%20Algorithms.pdf

GDPR Info. (n.d.). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Ghosh, M. (2025). Artificial intelligence (AI) and ethical concerns: a review and research agenda. *Cogent Business & Management*, *12*(1), 2551809. https://doi.org/10.1080/23311975.2025.2551809

Ijaiya, H. (2024). Harnessing AI for data privacy: Examining risks, opportunities and strategic future directions. *Int. J. Sci. Res. Arch*, *13*, 2878-2892. https://doi.org/10.30574/ijsra.2024.13.2.2510

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Office of the Parliament of Jamaica. (2020). The Data Protection Act, 2020 (Act of 2020). https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf

Polemi, N., Praça, I., Kioskli, K., & Bécue, A. (2024). Challenges and efforts in managing AI trustworthiness risks: a state of knowledge. *Frontiers in big Data*, *7*, 1381163. https://doi.org/10.3389/fdata.2024.1381163

Stewart, L. (2025). Exploring How Ai And Machine Learning Can Be Applied In Compliance

To Detect Anomalies And Predict Compliance Risks. *Available at SSRN 5249005*. https://dx.doi.org/10.2139/ssrn.5249005

Yazmyradov, S. (2024). A Comprehensive Review of AI Security: Threats, Challenges, and Mitigation Strategies. *The International Journal of Internet, Broadcasting and Communication*, *16*(4), 375-384. https://doi.org/10.17703/IJIBC.2024.16.4.375

Group Assignment 1: Developing a Security Policy for AI Enterprise Applications

Deliverable 2: Risk Analysis Matrix (Table Format)

Group Members:

Kaydeen Walker ID# 1902433

Alanzo Harris ID#2210195

Iyana Taylor ID#2209566

Lamar Eastman ID#2210172

Module Name: Computer Security

Module Code: CIT4020

University of Technology, Jamaica

Faculty of Engineering and Computing

School of Computing and Information Technology

Tutor: Kevin Johnson

Due: October 6, 2025

Risk Analysis Matrix

Summarising key risks, likelihood, impact, and mitigation strategies.

Risk Category	Description/ Threat Scenario	Likelihood (1-5)	Impact (1-5)	Mitigation Strategy
Data Privacy Risks	Employees might expose confidential or personally identifiable information (PII) when using external AI tools or LLMs. These platforms could retain or share that data, leading to privacy breaches, profiling, or unauthorized use.	4 - Good Chance	5 - High Impact	Classify and label all company data; prohibit uploading confidential data to public AI tools; use anonymization and encryption when processing sensitive data; maintain audit logs for every AI data interaction.
Access Control Issues	Without strong authentication and authorization controls, employees or external parties could gain unauthorized access to AI systems or data outputs, leading to misuse,	3 - Likely	4 - Medium Impact	Implement Role-Based Access Control (RBAC); enforce Multi-Factor Authentication (MFA); review and update access privileges regularly; restrict personal accounts for enterprise AI use.

	manipulation, or data theft.			
Model Integrity Risks	AI and LLM outputs can reflect bias, errors, or manipulation if the underlying data is poor-quality or poisoned. This could result in inaccurate decisions or harm to the company's reputation.	3 - Likely	4 - Medium Impact	Define approved use cases; require human review for critical outputs; test and validate models periodically to detect bias or drift; prohibit generation of discriminatory or misleading content.
Threat Mitigation Challenges	AI introduces new attack vectors like prompt injection, data poisoning, and model inversion that traditional defenses may not detect. Successful exploitation could compromise confidentiality, integrity, and availability.	4 - Good Chance	5 - High Impact	Monitor AI usage for anomalies; establish AI-specific incident response protocols; perform red-team and penetration tests; train staff to identify suspicious AI behaviors or outputs.
Compliance Risks	Failure to align AI use with legal requirements (e.g., Jamaica's Data Protection Act, GDPR)	3 - Likely	5 - High Impact	Ensure all AI tools and vendors meet compliance standards; maintain audit documentation; review

	could result in regulatory penalties, financial loss, and damaged trust with clients and partners.			compliance obligations annually; conduct regular system and policy audits.
Ethical Concerns	AI systems may produce biased or opaque outputs that reinforce unfairness, reduce transparency, or damage the company's credibility and customer relationships	3 - Likely	4 - Medium Impact	Establish an AI Ethics Committee; enforce fairness and transparency in AI operations; disclose AI-generated content in communications; prohibit discriminatory or biased outputs.

Risk Rating

Likelihood * Impact

Risk	Likelihood	Impact	Overall Rating	Priority
Data Privacy Risks	4	5	20	1
Threat Mitigation Challenges	4	5	20	1
Compliance Risks	3	5	15	2
Access Control Issues	3	4	12	3

Model Integrity Risks	3	4	12	3
Ethical Concerns	3	4	12	3

Note: To break ties in risk ranking, consider the *Impact* first (which would cause the most damage if it occurred), then consider the Likelihood if the Impact quantities are the same. Since these risks have the same Impact and Likelihood, prioritise by keeping them in the order they were calculated.