YORK College

CUNY The City University of New York

OFFICE OF INFORMATION TECHNOLOGY

AI Protocols and Best Practices Assessment and Compliance Framework

I. Introduction

- **Purpose:** Establish AI protocols and best practices at the College by leveraging the DOJ's *Evaluation of Corporate Compliance Programs* framework.
- **Scope:** Assess risks associated with the use of AI and other new technologies on legal compliance, mitigate negative consequences, and prevent reckless or deliberate misuse.
- **Compliance Objective:** Ensure AI usage aligns with criminal laws, institutional policies, and regulatory requirements (e.g., FERPA, HIPAA, GDPR).

II. Key Components of the AI Protocols and Best Practices Framework

1. **Oversight Structure and Accountability**

    - **AI Oversight Committee:** Create a body responsible for oversight of AI deployment and enforcement of standards.
    - **Accountability Mechanisms:** Define roles and responsibilities of executives, administrators, faculty, and IT stakeholders.
    - **Internal Reporting Channels:** Establish anonymous whistleblower channels for reporting misuse.

2. **Protocols and Best Practices Development and Risk Assessment**

    - **Adopt Best Practices:** Borrow elements from CUNY's standard computing use and cloud policy for alignment.
    - **Periodic Risk Assessments:** Conduct impact evaluations of AI technology on compliance and criminal law obligations (e.g., privacy breaches, fraud, bias).
    - **Stakeholder Consultation:** Include faculty, legal counsel, and IT security informulation and review of protocols and best practices.

III. Assessing Compliance with Criminal Laws

1. **Risk Identification and Impact Analysis**

    - **Privacy Violations:** Assess AI applications for compliance with privacy laws (e.g., FERPA for student records).
    - **Bias and Discrimination Risks:** Evaluate AI systems for unintended discrimination or biases in academic and hiring processes.

- **Fraud and Cybersecurity Risks:** Identify vulnerabilities that could enable insider fraud, phishing attacks, or data manipulation.

2. **Integration with University Policies and Procedures**

   - **Existing Policies Alignment:** Ensure AI systems align with acceptable use policies and ethics guidelines.
   - **Audit Mechanisms:** Build systems for monitoring AI outputs for legal or policy violations.
   - **Documentation and Transparency:** Maintain clear records of how AI models are developed, tested, and deployed.

IV. Mitigating Negative and Unintended Consequences

1. **Technology Testing and Evaluation**

   - **Pilot Programs:** Implement AI solutions on a trial basis before full deployment to identify potential flaws.
   - **Monitoring and Feedback Mechanisms:** Set up dashboards to track outcomes and flag issues in real-time.
   - **Bias Testing and Correction:** Regularly evaluate AI systems for unintended bias and improve algorithms as needed.

2. **Training and Awareness Campaigns**

   - **User Education:** Train faculty, staff, and students on the ethical and compliant use of AI systems.
   - **Awareness:** Conduct regular workshops on AI protocols and best practices and the consequences of misuse.

3. **External Auditing and Reviews**

   - **Third-party Audits:** Engage independent auditors to review AI systems and identify compliance risks.
   - **Compliance Scorecards:** Develop metrics to track adherence to governance standards and criminal law compliance.

V. Preventing and Mitigating Deliberate and Reckless Use

1. **Access Controls and Monitoring**

   - **Role-based Access:** Limit access to AI systems based on roles and responsibilities.

- **Behavior Monitoring:** Implement tools to detect unusual patterns or misuse by insiders.
- **Incident Response Plans:** Develop protocols to handle deliberate misuse, such as suspension of access or disciplinary action.

2. **Whistleblower Protections and Reporting Mechanisms**

- **Anonymous Reporting:** Provide safe channels for reporting misuse or unethical behavior.
- **Zero Retaliation Policy:** Ensure that individuals reporting concerns are protected from retaliation.

3. **Sanctions and Corrective Actions**

- **Enforcement Mechanisms:** Outline disciplinary procedures for reckless or malicious use of AI.
- **Corrective Action Plans:** Define remediation steps for addressing misuse or compliance violations.
- **Termination of Services:** Include clauses in contracts to terminate vendor agreements for non-compliance.

VI. Continuous Improvement and Program Evolution

1. **Ongoing Monitoring and Evaluation**

- **Periodic Reviews:** Regularly update the AI usage framework based on evolving laws, technology, and risks.
- **Metrics and Reporting:** Track metrics related to AI usage, incidents, and compliance status.
- **Adaptability:** Ensure policies are flexible enough to respond to new challenges or regulatory changes.

2. **Cross-Functional Collaboration**

- **Collaborative Governance:** Engage legal, academic, IT, and administrative units in reviewing AI protocols and best practices.
- **Engagement with External Experts:** Partner with legal and AI specialists to stay ahead of emerging risks and laws.

VII. Conclusion and Next Steps

- **Formal Adoption:** Finalize the AI protocols and best practices and seek approval from university leadership.
- **Implementation Plan:** Outline timelines and milestones for rolling out the framework.
- **Communication Strategy:** Share the protocols and best practices with the College community, emphasizing the importance of compliance and responsible use of AI.