POLICY TITLE
Responsible Artificial Intelligence (AI)

POLICY NUMBER
3-1007

Responsible Office: *Information Technology*	**Effective Date:** *6/10/2026*
Responsible Official: *Chief Information Officer*	**Last Reviewed Date:** *04/02/2026*
Policy Classification: *Finance and Administration*	**Origination Date:** *12/04/2025*

I. POLICY STATEMENT

Baton Rouge Community College (BRCC) is committed to the responsible, ethical, and secure use of Artificial Intelligence (AI) technologies. This policy establishes institutional standards ensuring that AI systems are used in ways that promote transparency, accountability, compliance, and human oversight. BRCC supports innovation while safeguarding privacy, data integrity, and institutional values. This policy shall be implemented in compliance with Louisiana Executive Orders JML 25-103 and JML 25-109, as applicable to AI platforms and data governance.

II. POLICY RATIONALE AND SCOPE

The purpose of this policy is to guide the responsible use of AI at BRCC in support of teaching, learning, research, and administrative operations. The policy governs the use of AI technologies including, but not limited to generative AI, machine learning, and automated decision-making tools.

III. POLICY AUDIENCE

This policy applies to all BRCC employees, contractors, vendors, and third parties who utilize AI systems or data owned, operated, or managed by the College.

IV. POLICY COMPLIANCE

All BRCC employees, contractors, vendors, and third parties are expected to comply with this policy and applicable state and federal regulations. Violations may result in disciplinary action, up to and including termination or contract revocation. Any suspected misuse, data breach, or non-compliance related to AI systems must be immediately reported to the Office of the Chief Information Officer (CIO).

V. POLICY DEFINITIONS

- **Artificial Intelligence (AI)**: Systems or software capable of performing tasks that normally require human intelligence, including but not limited to learning, reasoning, perception, cognition, planning, and problem-solving.

- **AI Hallucination**: A response generated by AI containing false or misleading information presented as fact.

- **AI Incident**: Any event where an AI system behaves unpredictably, is manipulated, or threatens compliance or security.

- **Confidential Data**: Information whose unauthorized disclosure could cause harm to BRCC or individuals.

- **Copyrighted Material**: Original works protected under federal law, where the creator holds exclusive rights to copy, distribute, or sell the work.

- **Ethical AI**: AI that promotes fairness, accountability, transparency, and privacy.

- **Generative AI**: Tools or systems used to create new content, such as text, images, or audio, based on existing data.

- **Machine Learning**: Systems that improve their performance through data analysis without explicit programming.

- **Proprietary Information**: Any code, formula, design, device, or process that constitutes proprietary or trade secret information submitted for official use or approval.

- **Responsible AI**: AI designed and used in ways that account for ethical, social, and organizational implications.

- **Restricted Data**: Data requiring strict adherence to federal, state, or local law, specific contractual agreements, or policy-based restrictions.

VI. POLICY IMPLEMENTATION PROCEDURES

A. **Governance:** BRCC shall maintain an Artificial Intelligence (AI) Governance Committee, chaired by the Chief Information Officer (CIO), responsible for institutional oversight, compliance, training, and risk management related to AI systems. Unless otherwise designated by the Chancellor, the CIO shall serve as the Institutional AI Liaison and shall ensure compliance with all LCTCS reporting requirements, including the submission of a list of vetted and approved AI platforms to the LCTCS Responsible AI Officer in accordance with LCTCS Policy 7.009.

B. **User Responsibilities**. Users shall familiarize themselves with the guardrails established in this policy. User responsibilities include, but are not limited to, the following:
    1. Complete AI training, as determined necessary by the governance committee.

2. All AI use must involve human oversight and validation of outputs for accuracy and integrity.
3. AI-generated content must be labeled appropriately when shared publicly. The label designating attribution may be made in the header, footnote, or by other appropriate placement or means.
4. AI may not be used as the sole source of decision-making or reference for institutional actions.
5. Users must immediately report any suspected data breaches or misuse to BRCC's CIO at it@mybrcc.edu, or by phone at 225-216-8267.
6. Users must opt out of data collection or model training features in AI systems when available.
7. BRCC email or credentials shall not be used to register unsupported or unapproved AI tools.
8. AI systems shall be used in accordance with data minimization principles, ensuring only data that is directly relevant and necessary is processed.
9. The Office of Chief Information Officer (CIO) shall identify data or information assets and classify such assets in accordance with their level of sensitivity. Questions regarding the classification of data as confidential, restricted, proprietary, copyrighted, and/or other classifications as required by federal and state law, as well as the CIO's data and information asset classifications.

C. **Prohibited Uses**. Employees may not:
1. Enter confidential, restricted, proprietary, or copyrighted BRCC data into unapproved AI systems.
2. Use AI to make autonomous decisions about enrollment, employment, program eligibility, compliance, or finances.
3. Employ AI systems operated by foreign nation-states or prohibited vendors, including systems affiliated with the Chinese Communist Party.
4. Generate or disseminate misleading, unlawful, hallucination, or discriminatory content.
5. Bypass or attempt to bypass AI safety or security controls (e.g., jailbreaking or generating malicious code).
6. Use AI to create, distribute, or assist in producing deepfakes, impersonations, misinformation, phishing, or other social engineering content.

D. **Reporting**. Employees must report suspected misuse, data breaches, or AI-related incidents to the CIO immediately.

E. **Training**. BRCC will provide regular training on responsible AI use. Training may include usage policies, best practices, data protection, risks, mitigation strategies, and ethics.

VII. POLICY RELATED INFORMATION

JML 25-103
JML 25-109
LCTCS Responsible, Ethical, and Secure Use of AI Policy
BRCC Information Security Policy

VIII. POLICY EXCEPTION

There are no exceptions to this policy.

IX. POLICY HISTORY AND REVIEW CYCLE

This policy shall be reviewed every three (3) years or as needed when technological, legal, or institutional changes warrant revision.

X. POLICY URL

This policy may be accessed on the BRCC website.

XI. POLICY APPROVAL

Willie E. Smith, Sr., Ed.D.	6/10/2026
Chancellor	Date
	Effective Date of Policy