Learning Management System (LMS) Access and Integration Policy

1. Purpose

This policy establishes requirements for vendors requesting access to the University of Detroit Mercy's Learning Management System (LMS) Blackboard. It ensures the protection of institutional data, compliance with security and accessibility standards, and adherence to FERPA regulations.

2. Scope

This policy applies to all third-party vendors requesting integration with the LMS, including cloud-based services, software applications, and external tools that require data exchange or authentication with the LMS.

3. Requirements for Vendor Integration

A. Security & Compliance Documentation

Vendors must provide the following documentation before access to the Blackboard server is considered:

1. **Higher Education Community Vendor Assessment Toolkit (HECVAT)** – A completed HECVAT Lite or Full version is required to assess the vendor's security posture and compliance with industry best practices.
2. **Voluntary Product Accessibility Template (VPAT)** – Vendors must submit a VPAT to demonstrate compliance with accessibility standards, ensuring compatibility with the Americans with Disabilities Act (ADA) and Section 508 of the Rehabilitation Act.
3. Disclosure of Data Use and Security Practices – Vendors must disclose:
    - The type of data collected, stored, or transmitted.
    - How data is secured and encrypted in transit and at rest.
    - Data retention and deletion policies.
    - Any third-party data sharing agreements.

B. Data Security & Protection

- Vendor systems must align with institutional cybersecurity policies and industry standards.
- Vendors are required to use institutionally managed system accounts or Single Sign-On (SSO) mechanisms (e.g., SAML and/or LTI 1.3) Learning Tools Interoperability (LTI) is preferred for authentication.
- Vendors should implement role-based access controls (RBAC) to minimize data exposure. Where applicable, third-party vendor systems should use dedicated integration accounts for LMS access to ensure the use of standard security practices.
    - The use of a university community member's user account for vendor LMS integration or access is strictly prohibited. Individual accounts are intended for personal use within the scope of the user's role.
- Regular security assessments and compliance reviews may be required as part of ongoing vendor management.

C. Compliance with FERPA

All vendor integrations must comply with the **Family Educational Rights and Privacy Act (FERPA)** to protect student records. Vendors must:

- Limit access to personally identifiable information (PII) to only what is necessary for service functionality.
- Not share or sell student data without explicit institutional approval.
- May be required to provide a Data Protection Agreement (DPA) outlining their commitment to FERPA compliance.

D. Institutional Review & Approval Process

1. Vendors must submit all required documentation to CETL for review.
2. A review will be conducted to evaluate security, compliance, and accessibility risks.
3. Approval from CETL is required before integration. Depending on the scope of the product, additional approvals from ITS may be required as well.

4. Periodic re-evaluation of vendor compliance may be required to maintain access.

4. Enforcement, Violations, Sunsetting

1. Failure to comply with this policy may result in the suspension or termination of vendor access to Blackboard.
2. Non-compliance with security or FERPA regulations may lead to further institutional action or reporting to regulatory authorities.
3. CETL may terminate vendor access without notification for use that exceeds the scope of approved access or after two consecutive terms of non-use.

5. Contact Information

For questions regarding vendor access and compliance, please contact CETL