

Standards and Procedures for Micro-Credentials

A Draft White Paper

Purpose

This document represents an addendum to the Micro-credentials Toolkit published by WVHEPC/WVCTCS in January 2026 and responds to Senate Bill 26-402.

Institutions are encouraged to develop, validate, issue, maintain, and share micro-credentials that recognize demonstrable competencies aligned with workforce needs, academic outcomes, professional standards, and lifelong learning objectives. Micro-credentials may be awarded to traditional students, nontraditional students, employees, or community learners who successfully demonstrate mastery of defined competencies.

Standards and Procedures for Identifying Appropriate Subjects and Skills for Micro-Credentialing

A. Standards for Selection of Subjects and Skills

Micro-credentials should be developed using the following criteria:

1. **Workforce Relevance**
 - Competencies address documented labor market demand.
 - Competencies align with employer-identified knowledge, skills, and abilities.
 - Competencies support industry-recognized certifications or licensure preparation.
2. **Academic Value**
 - Competencies support program learning outcomes.
 - Competencies represent discrete, measurable skills that can be assessed independently.
 - Competencies may stack into certificates, degree programs, or other credentials.

3. **Transferability and Scalability**
 - Competencies are applicable across multiple disciplines or industries.
 - Competencies support continuing education and lifelong learning pathways.
4. **Assessability**
 - Competencies can be measured using reliable and valid assessment methods.
 - Clear proficiency standards can be established.

B. Approval Process

1. Institutions will develop their own internal processes for approving micro-credentials submitted by academic departments, workforce programs, continuing education units, or approved institutional partners.
2. Each proposal may include:
 - Defined competencies;
 - Employer or industry validation;
 - Assessment methodology;
 - Learning pathway description;
 - Estimated learner effort;
 - Alignment to institutional and strategic priorities.
3. Institutions may choose to create Micro-Credential Review Committees consisting of representatives from:
 - Academic Affairs;
 - Workforce Development;
 - Institutional Effectiveness;
 - Information Technology;
 - Student Services; and
 - Appropriate industry stakeholders when applicable.

C. Demonstration of Mastery

A traditional or non-traditional student may earn a micro-credential through one or more of the following methods:

Direct Assessment

Learners demonstrate competency through:

- Performance-based assessments;
- Practical demonstrations;
- Simulations;
- Skills examinations;
- Competency-based evaluations;

- Industry certification examinations;
- Portfolio review.

Coursework

Learners may obtain a micro-credential by successfully completing designated coursework and achieving the established competency threshold.

Prior Learning and Experiential Learning

Learners may demonstrate mastery through:

- Professional experience;
- Military training;
- Industry certifications;
- Employer verification;
- Prior learning assessment;
- Portfolio submissions.

Required Level of Mastery

1. Each micro-credential shall establish defined proficiency criteria.
2. Competency standards must be measurable and documented.
3. A minimum mastery threshold should be established and published prior to issuance.
4. Assessment rubrics should be consistently applied and periodically reviewed for validity and reliability.

Standards and Procedures for the Design of Micro-Credentials

A. Design Standards

Each micro-credential should include:

1. Title and description;
2. Defined competencies and learning outcomes;
3. Assessment requirements;
4. Evidence of achievement;

5. Issuing department or authority;
6. Award date;
7. Expiration date, if applicable;
8. Metadata sufficient to verify authenticity and competency attainment.

The scope of a micro-credential should be sufficiently focused to represent a discrete set of competencies while maintaining meaningful value to employers and learners.

B. Validation Standards

Prior to issuance, every micro-credential should undergo validation to ensure:

1. Competencies are clearly defined and measurable.
2. Assessments accurately evaluate stated competencies.
3. Industry relevance is documented when workforce-focused.
4. Duplication with existing credentials is minimized.
5. Learning outcomes align with institutional academic standards.

Validation should occur:

- During initial development;
- At regular intervals thereafter; and
- More frequently when industry standards change.

C. Storage and Maintenance

1. All awarded micro-credentials should be maintained in a secure institutional repository, in compliance with applicable data privacy requirements.
2. The institution shall maintain:
 - Credential metadata;
 - Assessment records;
 - Issuance history;
 - Verification records.
3. Procedures shall exist for:
 - Credential correction;
 - Revocation when issued in error;
 - Renewal when expiration applies.

D. Access Standards

Authorized learners shall have continuous electronic access to their earned micro-credentials.

The institution shall provide mechanisms allowing:

- Viewing;
 - Downloading;
 - Verification;
 - Sharing with employers, educational institutions, and professional organizations.
-

Standards and Procedures for the Platform for Creating, Maintaining, Accessing, and Sharing Micro-Credentials

A. Platform Requirements

The selected platform for micro-credentials should:

1. Support creation and issuance of digital micro-credentials.
2. Maintain secure learner records.
3. Provide credential verification functionality.
4. Allow learner-controlled sharing.
5. Integrate with institutional information systems where feasible.
6. Support interoperability standards.
7. Provide reporting and analytics capabilities.
8. Meet accessibility requirements.

B. Technical Standards

The platform should support:

- Open Badge standards or equivalent interoperable frameworks;
- Secure digital authentication;
- Metadata-based verification;
- Audit trails;
- Secure cloud-based storage;
- Role-based administrative access;
- Data export capabilities.

C. Security and Privacy

1. The platform should comply with all applicable data privacy and security requirements.
2. Access controls should be implemented to protect learner records.
3. Credential integrity mechanisms should prevent unauthorized alteration.
4. Regular security reviews shall be conducted.

D. Governance and Oversight

Academic Affairs or some other unit at the institution should serve as the institutional authority for micro-credential governance and should:

1. Establish implementation procedures;
2. Monitor quality assurance;
3. Review credential performance and utilization;
4. Coordinate periodic program reviews;
5. Recommend modifications as workforce and educational needs evolve.

E. Recommended Operational Model

Institutions should consider employing a centralized digital credentialing ecosystem that:

- Uses a single approved credentialing platform;
 - Maintains a common institutional taxonomy for competencies;
 - Supports stacking of micro-credentials into certificates and degree pathways;
 - Enables employer verification through secure digital links;
 - Provides institutional reporting on learner participation, completion, and workforce outcomes.
-

Standards and Procedures for Verifying Completion of Micro-Credentials and Demonstrating Workforce Outcomes

Purpose

Institutions should establish standards and procedures to ensure that micro-credentials are awarded only upon verified completion of defined competencies and that such credentials contribute to demonstrable and measurable improvements in workforce participation, career advancement, and earnings.

Standards for Verifying Completion of Micro-Credentials

1. Defined Learning and Workforce Competencies

Each micro-credential should:

- Align with documented industry, workforce, professional, or occupational competencies.
- Include clearly defined learning outcomes that are measurable and assessable.
- Identify the specific knowledge, skills, and abilities demonstrated by credential recipients.
- Be mapped, where appropriate, to industry-recognized certifications, licensure requirements, workforce frameworks, or employer-validated competencies.

2. Assessment Requirements

Recipients should demonstrate competency through one or more of the following:

- Performance-based assessments.
- Industry certification examinations.
- Skills demonstrations or simulations.
- Portfolios evaluated using standardized rubrics.
- Clinical, laboratory, technical, or work-based learning experiences.
- Employer-validated projects or apprenticeships.

Successful completion should require achievement of established proficiency standards rather than participation alone.

3. Verification and Documentation

Institutions should maintain documentation supporting completion of each credential, including:

- Assessment results.
- Competency attainment records.
- Faculty or evaluator verification.
- Employer verification when work-based learning is included.
- Digital credential records and transcripts.

Each micro-credential should contain metadata identifying:

- Competencies earned.
- Assessment methods utilized.
- Date of completion.
- Issuing institution.
- Credit-bearing or non-credit status.

4. Quality Assurance Review

All micro-credentials should undergo periodic review to ensure:

- Continued workforce relevance.
- Alignment with employer needs.
- Appropriate assessment rigor.
- Consistency in credential issuance.

Reviews should occur at least every three years or more frequently when workforce demands necessitate modification.

Standards for Demonstrating Workforce Participation and Earnings Outcomes

1. Outcome Measures

Institutions should evaluate the effectiveness of micro-credentials using measurable workforce indicators, including:

- Employment placement rates.
- Workforce participation rates.
- Job retention rates.
- Promotion or advancement rates.
- Wage growth following credential attainment.
- Transition from unemployed to employed status.
- Transition from part-time to full-time employment.
- Entry into high-demand occupations.
- Continued enrollment in related educational pathways.

2. Data Collection

The institution should collect outcome data through one or more of the following:

- State workforce and unemployment insurance wage records.
- Graduate follow-up surveys.
- Employer surveys and feedback.
- Institutional student information systems.
- Workforce development agency partnerships.
- Third-party labor market data systems.

Data collection should occur at designated intervals, including as soon as six-months, one-year, and two-year post-completion periods when feasible.

3. Baseline and Comparative Analysis

To determine measurable improvement, institutions should compare:

- Pre-credential earnings to post-credential earnings.
- Employment status before and after credential completion.
- Outcomes of micro-credential earners relative to non-earners in similar populations when available.
- Credential-specific outcomes against institutional and regional workforce benchmarks.

4. Performance Thresholds

Each micro-credential should establish expected outcome targets appropriate to the occupational field, which may include:

- Employment placement benchmarks.
- Wage gain targets.
- Credential-to-employment conversion rates.
- Employer satisfaction measures.
- Skill utilization rates.

Programs falling below established performance thresholds should undergo review and improvement planning.

Procedures

Step 1: Credential Approval

Prior to implementation, each proposed micro-credential should:

1. Demonstrate workforce demand through labor market analysis.

2. Identify employer or industry validation.
3. Define measurable competencies and assessments.
4. Establish anticipated workforce outcome measures.

Step 2: Credential Issuance

Upon completion:

1. Faculty or designated evaluators verify competency attainment.
2. Assessment records are reviewed and approved.
3. The micro-credential is issued through the institution's credentialing system.
4. Credential metadata is recorded and maintained.

Step 3: Outcome Tracking

On an ongoing basis, the institution should:

1. Collect employment and earnings data for credential earners.
2. Analyze workforce participation and wage outcomes.
3. Compare outcomes to established benchmarks.
4. Prepare institutional effectiveness reports.

Step 4: Continuous Improvement

Results should be reviewed by appropriate institutional leadership and academic governance bodies to:

1. Identify high-performing credentials.
2. Revise or discontinue credentials with insufficient workforce value.
3. Update competencies to reflect industry needs.
4. Strengthen employer partnerships and workforce alignment.

Accountability and Reporting

Institutions should consider release of an annual Micro-Credential Effectiveness Report summarizing the following:

- Number of credentials awarded.
- Completion rates.
- Employment outcomes.

- Wage progression outcomes.
- Employer satisfaction findings.
- Recommended improvements.

The report shall be used to support institutional planning, accreditation, workforce partnership development, and continuous quality improvement efforts.

Success will be defined not only by micro-credential completion, but by evidence that credential recipients obtain meaningful workforce benefits, including increased employability, improved job performance, career advancement, and measurable earnings growth.

Draft Standards and Procedures for Record Retention, Storage, Security, and Learner Control of Micro-Credentials and Other Educational Attainments

Purpose

The following are draft standards and procedures governing the storage, maintenance, security, accessibility, and learner control of records related to micro-credentials and other educational attainments, including postsecondary certificates, degrees, professional licenses, industry certifications, apprenticeships, and workforce-based learning achievements. The draft is intended to promote portability, transparency, security, and lifelong learner ownership of educational records.

I. Authorized Entities for Storage and Maintenance of Records

A. Approved Record Holders

Records of micro-credential completion and related educational attainments may be stored and maintained only by authorized entities approved by an institution or a governing state authority.

Authorized entities may include:

1. The issuing institution of higher education.
2. The institution's official student information system.
3. A statewide credential repository approved by an appropriate authority.

4. Third-party digital credential providers operating under a written agreement with the institution.
5. State agencies responsible for workforce, licensing, apprenticeship, or educational records.
6. Consortium-based credential repositories authorized by participating institutions.

B. Requirements for Authorized Record Holders

Approved entities shall demonstrate the ability to:

- Maintain records in a secure digital environment.
 - Preserve records for long-term access.
 - Verify credential authenticity.
 - Protect educational records from unauthorized alteration.
 - Support interoperability among educational institutions, employers, and workforce agencies.
 - Comply with applicable data privacy requirements.
-

II. Comprehensive Learner Record

A. Unified Educational Achievement Record

Institutions may choose to maintain or participate in a system capable of storing educational achievements across an individual's learning lifecycle.

The record may include:

- Micro-credentials.
- Digital badges.
- Postsecondary certificates.
- Associate, bachelor's, master's, and doctoral degrees.
- Professional licenses.
- Industry-recognized certifications.
- Registered apprenticeship completions.
- Prior learning assessment awards.
- Military training equivalencies.
- Workforce training achievements.
- Continuing education credentials.

B. Interoperability

Records should be maintained in formats that facilitate:

- Transfer between institutions.
 - Employer verification.
 - State workforce reporting.
 - Transcript integration.
 - Digital wallet compatibility.
 - Future technology migration.
-

III. Record Retention Standards

A. Permanent Academic Records

Institutions shall maintain a permanent record of:

- Earned micro-credentials.
- Academic certificates.
- Degrees awarded.
- Credit-bearing competency achievements.

B. Record Preservation

Credential records shall:

- Remain accessible after graduation, separation, or retirement.
- Be maintained regardless of changes in technology platforms.
- Include sufficient metadata to verify authenticity and achievement.

C. Archival Requirements

Institutions should establish procedures to:

- Preserve historical credential records.
 - Protect against data loss.
 - Recover records in the event of system failure.
 - Ensure continuity during vendor transitions.
-

IV. Security Standards and Protocols

A. Security Framework

All entities maintaining credential records shall implement an information security framework that includes:

- Role-based access controls.
- Multi-factor authentication.
- Data encryption in transit and at rest.
- Routine security assessments.
- Continuous monitoring and logging.
- Incident response procedures.
- Data backup and recovery plans.

B. Credential Integrity

Systems shall employ mechanisms that:

- Prevent unauthorized modification.
- Validate issuer authenticity.
- Detect fraudulent credentials.
- Maintain audit logs documenting credential issuance, revision, and revocation.

C. Third-Party Vendor Requirements

Any contracted credential provider should:

- Meet institutional cybersecurity requirements.
- Undergo annual security review.
- Notify the institution of security incidents.
- Demonstrate compliance with applicable privacy and security standards.

V. Learner Ownership and Control of Records

A. Learner-Centered Principles

Individuals who earn micro-credentials and other educational attainments should retain primary control over the sharing and disclosure of their records, except where disclosure is required by law.

The system should be designed to promote:

- Learner ownership.
- Portability.

- Transparency.
- Consent-based access.

B. Access Rights

Students should have the ability to:

1. View all educational attainments contained in their record.
2. Download copies of their records.
3. Share credentials electronically.
4. Authorize third-party access.
5. Revoke previously granted access where technologically feasible.
6. Monitor access activity.

C. Selective Disclosure

Systems should allow individuals to share:

- A specific micro-credential.
- Groups of credentials.
- Individual certifications.
- Degree information.
- Workforce achievements.

...without requiring disclosure of unrelated educational records.

For example, a learner seeking employment in advanced manufacturing may voluntarily disclose a manufacturing safety micro-credential and apprenticeship completion record without disclosing unrelated academic information.

VI. Privacy and Consent Standards

A. Student Authorization

Except as permitted or required by law, educational attainment records shall not be disclosed without the student's informed consent.

Consent mechanisms shall:

- Clearly identify the information being shared.

- Identify the recipient.
- Specify the duration of authorization.
- Permit withdrawal of consent.

B. Compliance Requirements

Institutions and authorized entities should comply with:

- The Family Educational Rights and Privacy Act (FERPA).
- Applicable West Virginia privacy laws.
- State cybersecurity requirements.
- Institutional records-retention policies.

C. Data Minimization

Only information necessary to accomplish a legitimate educational, employment, credential verification, or regulatory purpose shall be disclosed.

VII. Verification and Employer Access

A. Credential Verification

Authorized employers, licensing boards, workforce agencies, and educational institutions should be able to verify credentials through secure methods, including:

- Verification URLs.
- Digital signatures.
- Credential identification numbers.
- Secure learner-authorized access portals.

B. Fraud Prevention

Verification systems should be designed to:

- Confirm credential authenticity.
 - Identify revoked credentials.
 - Prevent credential duplication.
 - Detect unauthorized alterations.
-

VIII. Governance and Oversight

A. Institutional Responsibilities

Each institution should designate a responsible office, such as the Registrar, Information Technology Division, or Office of Academic Affairs, to oversee:

- Credential record maintenance.
- Security compliance.
- Vendor management.
- Privacy protections.
- Learner access procedures.

B. Annual Review

Institutions shall conduct an annual review of:

- Security controls.
- Learner access functionality.
- Vendor performance.
- Compliance with state requirements.
- Record retention practices.

C. Continuous Improvement

Institutions shall periodically evaluate emerging technologies and standards that improve:

- Credential portability.
- Identity verification.
- Learner control.
- Data security.
- Employer acceptance.