Integrity Advocate

IACET Standard Guidance:

Safeguarding the Integrity of Continuing Education and Training in the AI Era

Introduction

In an increasingly digital world, the shift to online delivery of continuing education and training has brought new challenges to maintaining the integrity of learning environments.

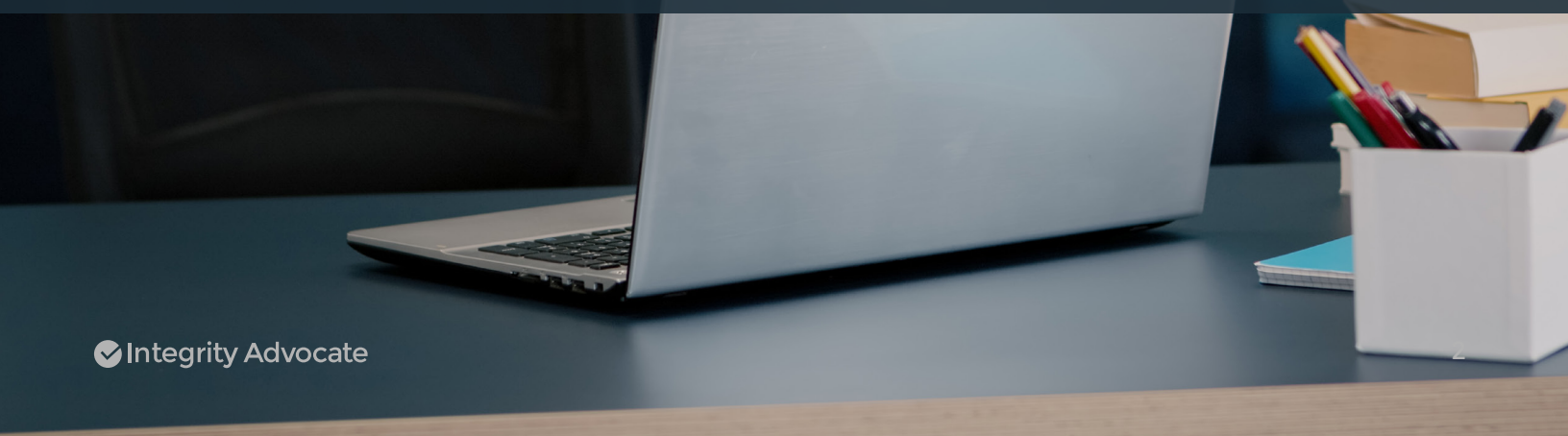
Specifically, the increasing prevalence of automated tools, such as GPT-powered browser plugins, has raised questions about how best to ensure that participants in training programs are genuinely engaged, and their identities verified throughout the process. The International Association for Continuing Education and Training (IACET) and other regulatory organizations are reevaluating their standards to address these concerns.

This paper outlines practical guidance for organizations accredited by IACET and similar bodies to ensure the trust and credibility of their online continuing education programs.

By doing so, organizations can continue to fulfill their crucial role in maintaining public confidence in training as a tool for risk mitigation, regulatory compliance and professional development.

Who We Are

Integrity Advocate is built on a deep understanding of risk mitigation, compliance and training technologies. Our mission is to protect the integrity of accreditation, certification and qualification systems by helping training organizations develop robust processes to accommodate the increasing prevalence of online learning.



The Importance of Integrity

In professions where public safety is a concern, the knowledge and skills acquired through continuing education can be a matter of life and death. When organizations fail to uphold the integrity of their training programs, the consequences can be catastrophic.

Integrity Advocate was founded after Robert Day witnessed firsthand how inadequate training led to a tragic accident in which two individuals were severely burned. The incident resulted in legal charges against the responsible company, and undermined confidence more broadly in the organization's training and certification systems.

This example underscores the vital role that continuing education plays in risk mitigation and regulatory compliance. To protect public safety, uphold their reputations, and meet legal and regulatory requirements, organizations must ensure that their training programs maintain the highest standards of integrity.

AI Plug-ins: An Emerging Threat

The rapid rise of AI technologies, such as GPT-powered plugins, has introduced significant challenges to maintaining the integrity of online learning and assessments.

The challenge for accrediting bodies like IACET is to ensure that training and assessments remain credible and compliant with evolving standards, despite the increasing sophistication of AI tools.

GPT-powered plugins — often marketed as 'study aids' or 'learning helpers' — can be installed within browsers and used to automatically complete assessments on a learner's behalf. Tests have shown that these plugins can answer hundreds of questions within seconds.

This has led to an environment in which anyone — even, as we've demonstrated in the past, a dog — can successfully complete online CEUs and obtain certifications without the required training. Needless to say, this has serious implications for the integrity of professional development and assessment.

Organizations must adapt their systems and safeguards to address the risks posed by AI. By implementing robust identity verification and participation monitoring, organizations can ensure that their training programs continue to meet the rigorous standards required for public trust and regulatory compliance.

Applicability

The below guidance is applicable to any organization that adheres to ANSI/IACET 1-2018 Standard for Continuing Education and Training. Additionally, it meets requirements spelled out in IACET's Petroleum and Natural Gas Industry Criteria for Continuing Education and Training.

Whether in the energy sector or general continuing education, the implementation of these practices will ensure that participation records accurately reflect compliance with regulatory and accreditation standards. By doing so, organizations can protect the credibility of their programs and prevent the issuance of fraudulent credentials.

Guidance on Meeting the Intent of Standard 8.1

> *The Provider shall have a process verifying that the learner who registers and participates in the learning event is the same learner who receives the IACET CEU.*

This standard applies to in-person, hybrid and online training environments. Like all IACET standards, it is focused specifically on outcomes, and leaves it to organizations to determine the appropriate steps to maintain compliance.

With that in mind, we've prepared the following section to outline our recommended best practices for IACET 8.1 compliance in the age of AI.

In-Person Identity Verification

For in-person training sessions, IACET 8.1 requires that each organization have a process in place for verifying a participant's identity. The same level of verification is not needed for all industries and businesses; organizations may decide based on their specific needs, industry requirements and risk profile.

For example, an organization that only trains internal employees on low-risk protocol might be fine using an employee ID as verification. However, a governmental unit delivering training on classified subjects might require biometrics for its verification process.

For most medium-to-high-risk applications, a reasonable compromise between these extremes may involve verification using an official government ID that is confirmed at the time of the learning event.

Acceptable Forms of ID

Accredited organizations are not required to verify the authenticity of an ID beyond a reasonable standard that aligns with other industries. The US Transportation Security Administration (TSA), for example, recognizes expired government-issued IDs as valid for identity verification purposes, so long as they contain accurate identifying information.

This pragmatic approach helps organizations maintain integrity while avoiding unnecessary logistical hurdles in the verification process.

Online Identity Verification

In online training environments, the same standards apply. Organizations must have a process in place for verifying learner identity that is appropriate to the level of risk should the CEU be awarded to the wrong person.

Superficial security measures, including honor statements, usernames/passwords, and even two-factor authentication, are easy to circumvent. These methods do not confirm the individual's identity throughout the learning event and, as such, they may not be stringent enough to conform to the intent of IACET 8.1, particularly for high-risk continuing education applications.

Concerns with GPT Plug-ins and Verified Participation

The rapid advancement of GPT-powered plugins poses significant threats to maintaining the integrity of online assessments. As noted above, these tools can complete assessments without the learner's input, allowing participants to bypass the educational process entirely. (Additionally, these plugins pose a risk to proprietary content, as they can extract questions and store them for future use by third parties.)

Organizations must implement safeguards that detect and prevent the use of AI tools during assessments. These unsanctioned "study aids" enable learners to access assessment content without engaging in the learning process or compensating the accrediting organization.

We recommend restricting the use of browser plug-ins during exams, or using AI detecting/blocking software to flag instances of noncompliance.

Notice on Participation

On September 17, 2024, IACET issued an industry notice encouraging member organizations to:

> *Consider implementing tools that can monitor participation through video and detect whether AI tools are being used to complete the course on behalf of the learner.*

With the rise of AI-based technology, participation verification is more than simply confirming attendance or superficial engagement. Clicking through content, using time-based restrictions, or employing other passive methods may not meet the standard's intent, as they fail to verify that the participant is actively engaged or that their identity is continuously confirmed during the session.

Similar to in-person events, participants that are distracted (e.g., using social media, watching movies or engaging in unrelated activities) would not be considered to be demonstrating genuine participation. The same logic applies to online sessions — screen activity alone may not offer sufficient proof of engagement.

Our recommendation is that organizations implement a process to ensure, based on their level of risk tolerance, that:

- Verified individuals are engaged throughout the learning modules or assessments
- Random checks or key participation points are used to re-verify identity and monitor engagement

Applicability of Requirements

The requirement to verify identity and participation is directly linked to learning outcomes and is often reflected in the wording of completion records. For example, if a participant receives a certificate stating they have 'completed,' 'achieved,' or 'participated' in an event, this implies that their identity and participation have been verified.

Failure to meet these standards can result in legal action, as organizations have been charged with issuing fraudulent documents when such claims were unsubstantiated.

Organizations should consider alternative wording on certificates when identity and participation are not meant to be implied. Phrases such as 'was awarded' or 'has received' can be used to prevent misleading claims about the level of participation or verification involved.

Applicability Based on Risk

In many cases, the learning content associated with CEUs has legal, regulatory or risk mitigation implications. For content that contributes to maintaining a professional designation or fulfilling a regulatory requirement, strict identity verification and participation standards must be applied.

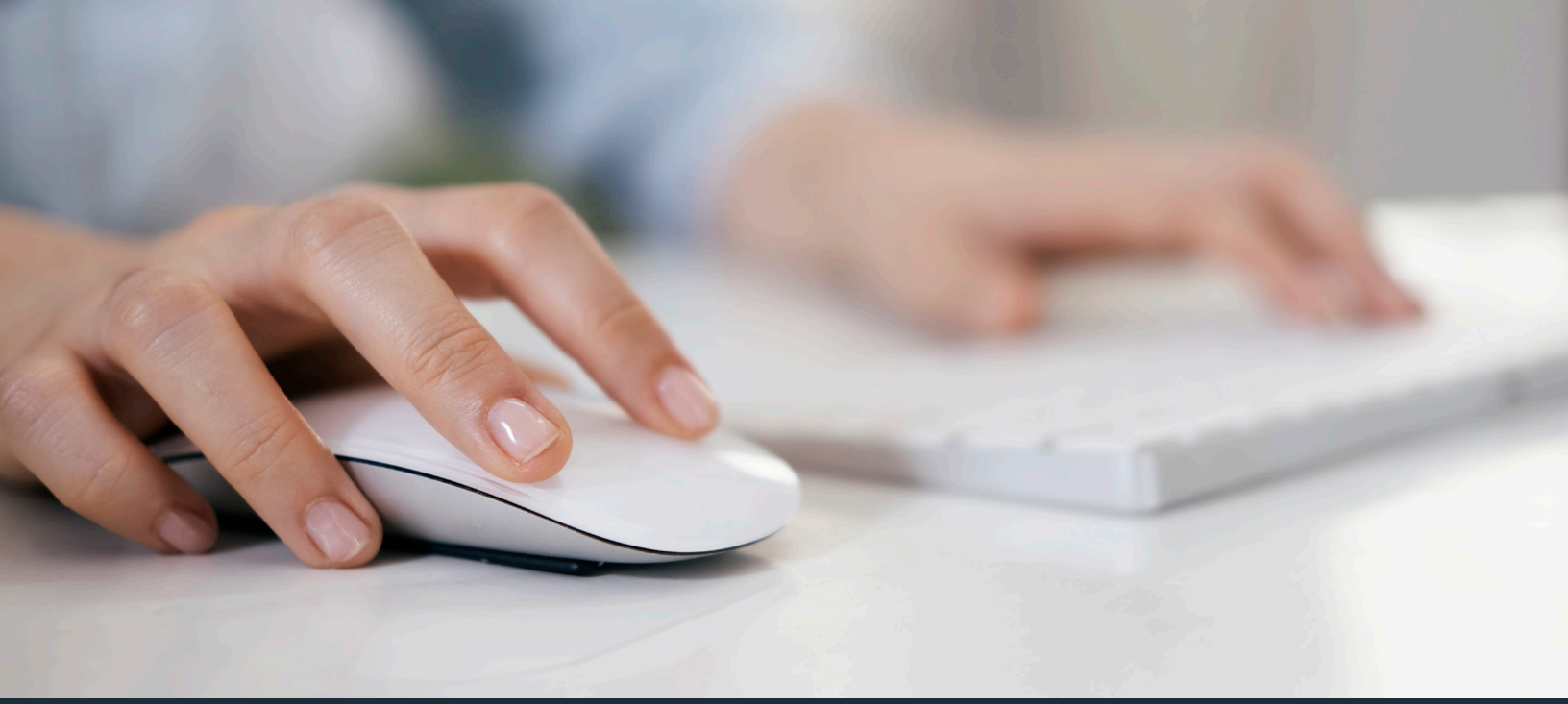
For low-risk learning content that does not mitigate risk and/or contribute to legal or regulatory compliance, organizations may establish alternative processes for awarding CEUs. In such cases, the record of achievement should reflect that the award was not based on verified participation or completion.

Undue Hardship as a Reason for Noncompliance

There may be instances where organizations are unable to meet the requirements of 8.1 due to financial or operational challenges. 'Undue hardship' refers to situations where compliance with the standard would create an excessive financial burden, making it unreasonable for the organization to meet the requirement.

To claim undue hardship, organizations must provide specific evidence, including:

- **Cost analysis:** A detailed breakdown of the projected costs for meeting the standard compared to the organization's financial capacity. This analysis should demonstrate that compliance would create an unreasonable financial strain.
- **Exploration of alternative solutions:** Documentation showing that lower-cost solutions were considered but found to be unfeasible. This demonstrates the organization's good faith effort to comply with the standard.



Conclusion

The purpose of this document is to provide accredited organizations with practical steps to safeguard the integrity of their continuing education and training programs.

Ensuring that professionals acquire the necessary skills and knowledge to perform their roles safely and effectively is essential. As AI technologies, such as GPT plugins, pose new risks to online learning, organizations must adopt strong measures to protect the credibility of their programs.

By adhering to the guidance outlined in this white paper and meeting the standards of ANSI/IACET 1-2018, organizations can maintain trust in continuing education units (CEUs) and uphold the quality and integrity of professional development.