

April 2025

Appendix 1: Mechanism for Preventing Identity Theft and Verifying Trainee Work

v1.0

ICE Arabia for Training (Saudi Arabia)

Table of Contents

1. Purpose	2
2. Identity Theft Prevention Measures	2
2.1 Secure Access Controls	2
2.2 Monitoring Access Patterns	2
2.3 Identity Validation	2
3. Mechanisms to Verify Trainee Work and Prevent Fraud	3
3.1 Randomized Assessments	3
3.2 Safe Exam Browser (SEB)	3
3.3 Anti-Plagiarism Tools	3
4. Continuous Monitoring and Reporting	3
5. Review and Improvement	4

1. Purpose

This document details the procedures implemented by ICE Arabia for Training ("ICE") to prevent identity theft in the e-learning and training environment and to verify the authenticity of trainees' work.

2. Identity Theft Prevention Measures

ICE applies robust mechanisms to safeguard the integrity of trainee identities throughout their learning journey:

2.1 Secure Access Controls

- Unique, non-transferable login credentials are issued to each trainee.
- Regular monitoring and periodic mandatory password updates are enforced.

2.2 Monitoring Access Patterns

- Learning management system logs access locations, IP addresses, and timestamps to detect irregular access patterns that may indicate impersonation.

2.3 Identity Validation

- At enrollment and prior to assessments, trainees are required to provide valid government-issued identification.
- Proctoring software may be used where applicable to verify identity during online exams.

3. Mechanisms to Verify Trainee Work and Prevent Fraud

ICE employs multiple strategies to verify the authenticity of submitted work:

3.1 Randomized Assessments

- Assessments are generated dynamically using a randomized question bank, ensuring that no two exams are identical.

3.2 Safe Exam Browser (SEB)

- Exams are administered through Safe Exam Browser, locking down devices and disabling navigation, screen sharing, copying, pasting, and internet disconnection during the test session.

3.3 Anti-Plagiarism Tools

- Assignments are subjected to plagiarism detection software to identify unoriginal content or improperly cited materials.

4. Continuous Monitoring and Reporting

- Regular audit trails are maintained for all assessments and submissions.
- Staff are trained to identify signs of academic dishonesty or identity misrepresentation.
- Any suspicious activities are flagged, investigated, and recorded.

5. Review and Improvement

- Mechanisms are reviewed annually to ensure their effectiveness and compliance with evolving e-learning best practices.
- ICE remains committed to adopting new technologies and strategies to uphold academic integrity.

This document must be read in conjunction with ICE's Academic Integrity and E-Learning Fraud Prevention Policy v1.0.

This policy can be changed by Management from time to time.