CANADA'S OIL & NATURAL GAS PRODUCERS

Guide

Online Training Identity Verification and Remote Proctoring

June 2018

2018-0022

The Canadian Association of Petroleum Producers (CAPP) represents companies, large and small, that explore for, develop and produce natural gas and crude oil throughout Canada. CAPP's member companies produce about 80 per cent of Canada's natural gas and crude oil. CAPP's associate members provide a wide range of services that support the upstream crude oil and natural gas industry. Together CAPP's members and associate members are an important part of a national industry with revenues from crude oil and natural gas production of about $110 billion a year. CAPP's mission, on behalf of the Canadian upstream crude oil and natural gas industry, is to advocate for and enable economic competitiveness and safe, environmentally and socially responsible performance.

2100, 350 – 7 Avenue S.W.
Calgary, Alberta
Canada T2P 3N9
Tel 403-267-1100
Fax 403-261-4622

1000, 275 Slater Street
Ottawa, Ontario
Canada K1P 5H9
Tel 613-288-2126
Fax 613- 236-4280

1004, 235 Water Street
St. John's, Newfoundland and Labrador
Canada A1C 1B6
Tel 709-724-4200
Fax 709-724-4225

360B Harbour Road
Victoria, British Columbia
Canada V9A 3S1
Tel 778-410-5000
Fax 778-410-5001

Overview

Online training is often used by employers to develop competencies in their staff. However, with this convenience comes the need to verify online training has been reliably delivered to the intended employee. Without reliable verification, employers incur serious legal and other risks associated with inadequately trained staff. This document describes online training identity verification and remote proctoring (IVRP), the legal, regulatory, and technological considerations of using IVRP, and provides best practices to improve IVRP in the workplace.

Contents

1 Introduction

Online training has consistency, engagement, cost, and efficiency benefits. The challenge for employers using numerous types of online training is that they do not know who is completing the training nor the level of participation or attention it is given.

As industry training may be both a regulatory requirement and a mitigative measure to address significant operational risks, it is vital that employers can verify that the intended personnel received the online training, and that they participated in it as intended.

In contrast, instructor-led training can both verify the identity of participants (by checking identification), and monitor participation to established standards through instructor/learner interactions.

In most cases, the standard used for instructor-led was not upheld when the same educational material was completed online. Identity verification and remote proctoring (IVRP) for online training can meet this standard but was originally considered unreasonable due to technology limitations and cost. Fortunately, web-enabled IVRP is now more accessible and economical to a point where widespread application of this technology is possible.

IVRP technology is particularly critical when organizations use online training as part of risk control strategies that seek to ensure employees are competent in regulatory critical activities (e.g., standards of business conduct, financial accounting requirements, reporting requirements, disclosure, health and safety or environmental requirements).

To safeguard the integrity of online training, this guide has been developed to provide organizations with the information needed to ensure the methodology and technology chosen to administer IVRP meets organizational needs and legal requirements, including future due diligence defence needs.

1.1 Background

CAPP's *Enabling Zero* strategy includes the development of a consistent systematic approach to assure the upstream oil and gas operations are planned and executed by competent personnel. Given the increasing importance of online training to competency development, ensuring robust IVRP is an essential part of the overall *Enabling Zero* strategy.

Underpinning the strategy, and this guide, are the moral and regulatory requirements for all employers to reduce the risks associated with the delivery of their products and services. Many of these risks are mitigated by personnel with specific competency requirements often requiring years to develop and necessitating accurate and reliable verification.

While developing competencies is facilitated by online training, online training remains only one element of competency development. The value of both experiential and social learning, for example, in competency development can be seen in the 70/20/10 model. The 70/20/10 model can be explained as;

70% - Experiential/Experience - learning and developing through day-today tasks, challenges and practice

20% - Social/Exposure - learning and developing with and through others from coaching, exploiting personal networks and other collaborative and co-operative actions

10% - Formal/Education - learning and developing through structured courses and programs

As training may only represent 10 per cent of the process utilized by organizations to develop workforce competency, it is important that the training conducted is of good quality and received by the personnel requiring it. Organization records of specific personnel participation in training may be relied upon as evidence of due diligence efforts post incident.

Where formal training is being conducted, employers need to ensure it is received by the personnel that require it and that those same personnel are participating in the training. The identification and participation of participants in training is easily managed in instructor-led training but when the training is delivered online significant challenges exist. This challenge is the purpose for this guide.

1.2 Acknowledgements

The creation of this document would not be possible without the permission from the Industrial Occupation Safety and Health Association of Alberta (IOSH Alberta) Executive to utilize the IOSH *Best Practice on Web-Based Training, Identity Verification and Proctoring* (2015) and incorporate into this guidance. IOSH Alberta consists of companies engaged in various aspects of industry health and safety management in Alberta. Formed in the late 1960's as a medium for sharing information and discussing possible resolutions of occupational health and safety problems in the industry. In 2018, there are approximately 40 member companies.

The creation of this document was also benefited by the involvement of the Chartered Professionals in Human Resources executive membership. CPHR Alberta is the professional association dedicated to strengthening the human resources profession and upholding the highest standards of practice. With 6,000 members in major cities across Alberta, the Northwest Territories and Nunavut, CPHR Alberta is the third largest HR Association in Canada. CPHR Alberta is the exclusive registration body in Alberta for the Chartered Professionals in Human Resources (CPHR) designation, which is the professional standard in Canada. The CPHR demonstrates HR expertise, experience and ethical management of today's human capital.

1.3 Legal Disclaimer

This Industry Best Practice is not intended to constitute legal advice. It is intended to be used as a guideline of best practices to assist organizations using or considering online training as part of their education and training requirements. The specific laws with respect to environment, OHS and privacy vary over time and differ from jurisdiction to jurisdiction. Legal matters are often complicated and highly dependent on the specific circumstances of each case and laws from that jurisdiction.

Organizations should seek legal advice based upon the specific circumstances of their matter from a competent lawyer fully licensed to practice in the particular jurisdiction and knowledgeable of the area of law in question.

1.4 Scope

Using online training to deliver health and safety training content is a growing practice that benefits both employers and employees. According to the 2011 Workplace Employment Relations Study, 70 per cent of workplaces provide online health and safety training to experienced employees, and 83 per cent of workplaces provide online induction training to new recruits.

This guide applies to employers delivering training online, and is particularly important if that training is related to critical roles and competencies (see CAPP's *Critical Roles and Competency Guide*).

2 Definitions

Due Diligence Defence is a legal defence available to a company or person charged with a strict liability offence. Most regulatory offences are strict liability offences, which includes most environmental and Occupational Health and Safety offences. The defence is available even when a breach of a strict liability offence has occurred. It provides the defendant with an opportunity to defend against charges by proving it was duly diligent in preventing the breach. The defence requires the defendant to prove on a balance of probabilities that all reasonable care was exercised in the circumstances. This often means organizations must prove a proper system was established to prevent the breach and that reasonable steps were taken to ensure the effective operation of the system.

Identity Verification is the confirmation of an individual's identity through comparison of the provided name and facial characteristics of the individual in a digital image compared with a credible form of photographic identification or a previously identity confirmed digital image.

Facial Recognition is an automated technological process that utilizes facial characteristics to identify and/or verify the individual’s identity or presence.

Remote Proctoring is the use of web-enabled technology to supervise an examination or delivery of training materials. This could be through live monitoring, recorded session monitoring, biometric face tracking technology, or a combination thereof.

Web-enabled means any software or application that relies on or runs within a web browser without the need for additional download or installation on the receiving device.

Regulatory Critical Training Materials are those which organizations use as they seek to ensure employees, volunteers or members possess competence in order to meet legal and/or regulatory obligations.

3 Current Practice

Many organizations using online training for Regulatory Critical Training materials rely on usernames and passwords to restrict/grant access to online training. As usernames and passwords are easily and often shared this login step does not confirm identity or participation, and is not a deterrent against training integrity violations. Other progressive organizations have opted to use supervised computer labs to create a secure environment and requiring the presentation of government issued photo identification to gain access.

3.1 Identity Verification and Remote Proctoring (IVRP)

Organizations currently using IVRP are most commonly post-secondary institutions. These institutions mandate software that typically allows students to complete an activity or examination in a virtual meeting with a person (a proctor). The software allows the proctor to view the student through their web camera, validate the student's identity through the viewing of accepted identification and monitor their activities to ensure acceptable standards are maintained (no outside assistance or proxy).

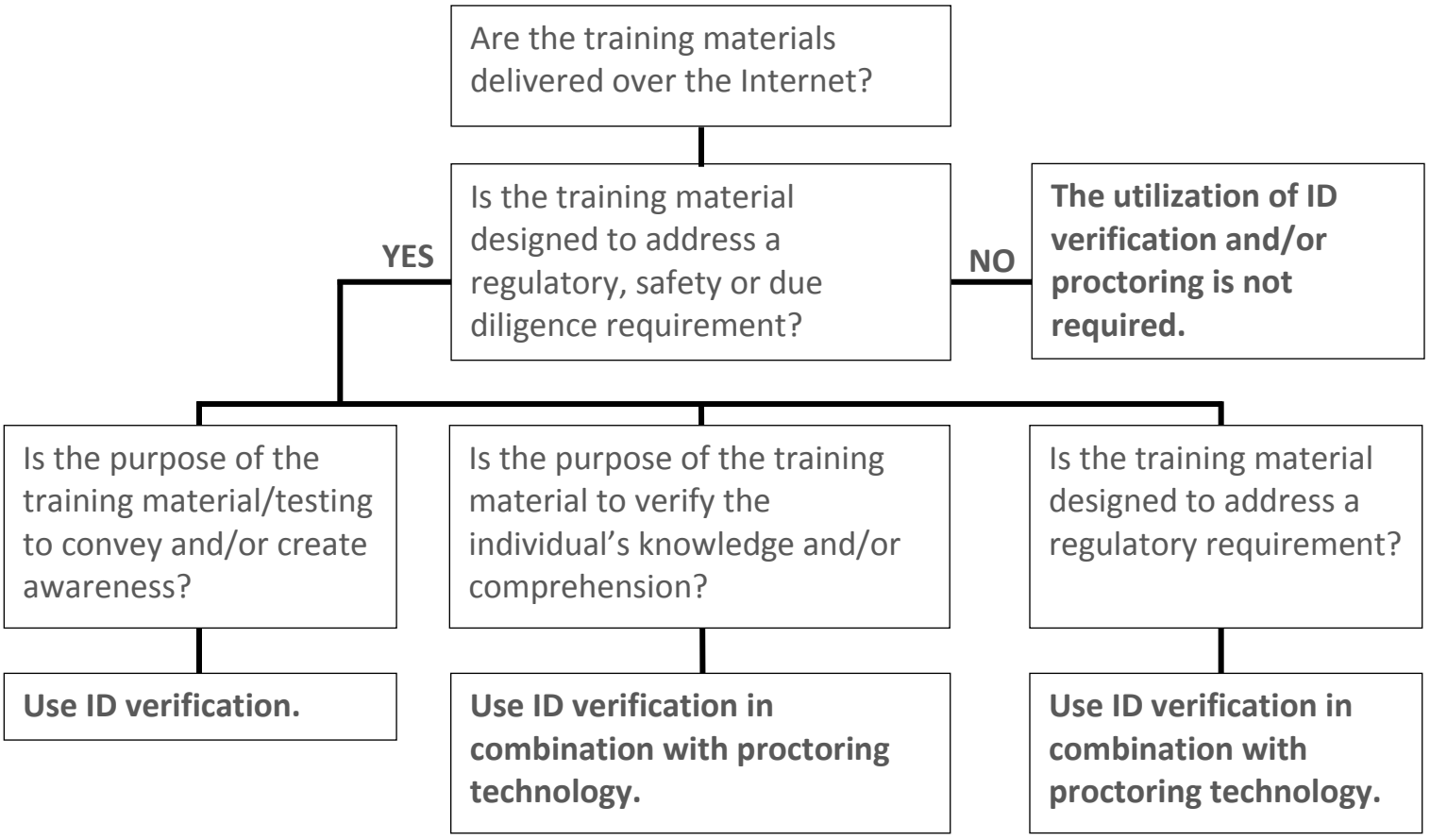
4 Legal and Regulatory Considerations

4.1 Use of Web-enabled Electronic Identity Verification and Remote Proctoring

All organizations are under obligation to comply with the rules that govern their activities. These rules may be in the form of policies or law and may be enforced by industry regulators. For example, two areas that all organizations are required to comply with are Occupational Health and Safety, and Environmental regulations. The consequences of an individual and/or organization breaching regulatory requirements from the above two areas are severe and can result in fatalities, lifelong disablement, property damage, environmental contamination, extreme financial penalties, lawsuits, criminal liability, and potentially, the insolvency of the organization.

Therefore, organizations must ensure that their representatives (i.e., employees, contractors, subcontractors, agents, volunteers or members) are competent to meet obligations and avoid breaches. Part of the proof of competence necessitates proving the person alleged to be competent received the training and demonstrated competency in the area in question. Given the significant risks involved, organizational use of web-enabled identity verification and/or proctoring can be a critical element in discharging the burden on an organization to prove competency of an individual or management team. Figure 4-1 provides the rationale of when and what aspects of the technology to use.

Figure 4-1 Utilization Rationale



4.2 Due Diligence

4.2.1 Due Diligence Defence

An organization potentially in breach of a strict liability offence may rely on a due diligence defence in order to avoid liability for the breach. Once the breach is proven by the prosecution, the burden of proof shifts to the organization to establish, amongst other things, that a formal system was adopted and the organization took reasonable steps to ensure the effective operation of the system[1]. If the organization fails to discharge its burden of proof, then a conviction will result. Although the system is subject to technological limitations[2], given advances in internet technology, the benchmark for technological limitations in relation to web-enabled IVRP has shifted and a new standard has been set.

Courts and prosecutors will assess the actions and omissions taken by an organization to prevent an incident in terms of what is "reasonable" in the circumstances. This assessment involves a contextual examination including amongst other things, examining what technology or engineering was available that would have prevented the incident or reduced its likelihood. If technological or engineering advancements are economical and readily available, and an organization does not use such tools, then the defence of due diligence is weakened and the organization is exposed to liability. In this instance, given technological advances which make the use of web-enabled IVRP economical and reliable, such systems should be incorporated into the delivery of, and associated examinations for, web-enabled training materials.

4.2.2 Due Diligence Case Study

The Alberta case of R. v. Rose's Well Services Ltd[3] provides an example of both the identity verification problem, and the remote proctoring problem. In that case the employer was convicted of OHS offences after two workers were badly burned in a fire while off-loading hydrocarbons from a tanker truck. The workers were filling a metal storage tank from their tanker truck when fumes from the process were ignited by the engine of the truck. The driver had parked the tanker truck too close to the metal storage tank and the engine from the truck provided the ignition source for the fumes that had gathered from the process. The employer, as part of its due diligence defence, called evidence that its employees had taken the Petroleum Safety Training program ("PST") offered by Energy Safety Canada (an industry training organization). This was an online training program which provided basic safety training for workers in the oil and gas industry, and while not directly on point in terms of the fire in question, it was a

[1] R. v. Bata Industries Ltd. (1992), 7 C.E.L.R. (N.S.) 245, 9 O.R. (3d) 329, 70 C.C.C. (3d) 394 (Prov. Div.)
[2] R. v. Commander Business Furniture Inc. (1992), C.E.L.R. (N.S.) 185 (Ont. C.J.)
[3] R. v. Rose's Well Services Ltd. (Dial Oilfield Services), 2009 ABQB 266

component of the health and safety management system used by the employer and part of its due diligence defence.

At trial the driver of the tanker truck testified he had helped his co-workers through the online PST training program and had even answered the exam questions for many of them. Needless to say this came as a surprise to the defendant employer who discovered this fact for the first time at trial. The employer had naively assumed the training they were paying for was being taken by the employees intended. In effect, the driver and his co-workers circumvented the intent and purpose of the training and denied the employer any return on that safety investment. At the time there was no identification method used to ensure the identity of the person taking the exam nor any proctoring system of the exam to stop such behavior. This was a proof problem for the employer, which is significant given the fact there is often a reverse onus of proof on the employer to prove all reasonable care was taken in the circumstances.

4.3 Paramountcy of Engineering Controls

Most jurisdictions in Canada have adopted a hierarchy of elimination and control measures for workplace hazards which vary from engineering, administrative, personal protective equipment, or a combination thereof, e.g., Alberta OHS Code Part 2, 9(1). What is clear from these legislative requirements is that engineering controls are placed at the top of the hierarchy. Accordingly, organizations are legislatively required to eliminate or control hazards with engineering methods providing they are reasonable, which by extension includes computer engineering. Organizations which fail to adopt technological advancements that are readily available and economical are vulnerable to breaching this hierarchy of control measures.

4.4 Privacy Considerations and Best Practice

In addition to compliance with jurisdictionally specific privacy requirements international privacy compliance must be attained as the very nature of web-based access to educational material creates the opportunity for utilization across multiple jurisdictions[4].

Where technology is integrated into an online training process that verifies the identity and participation of personnel taking on-line training/testing, specific privacy considerations must be addressed.

Information Collection/Segregation: If media is captured of the individual's government issued identification and media of an individual and what may be a home environment should not be collected by or accessible to an entity that holds other personal information on the individual that would create an increased risk to the individual in a situation where the personal information may be viewed together. For example, the name, image and interior images of a home and individuals within it has limited privacy

[4] Getting the Deal Through, Data Protection & Privacy in 26 Jurisdictions Worldwide, 2014, Contributing editor: Rosemary P Jay

impact until the information is combined with an individual's address, phone number, employer and deductive information such as shift schedule[5].

Media images of Government Identification and Participation: Personnel that provided reasonable access to their image for the purpose of identity and participation verification of an online course/exam may also be inadvertently providing media that is personal in nature, indicate lifestyle, religious, ideological choices that they did not intend for disclosure and that could have a potential impact on their employment relationship. To eliminate an impact on employment relationships all media should be kept inaccessible to the employer, employer associations and agents and deleted within twenty-four hours of collection if not required to demonstrate their identity of to document non-compliance[5].

Additional privacy requirements for web-enabled IVRP should include[6]:

1) Persons subject to IVRP must be provided with the privacy policy and instructions for use in a language they understand.
2) The information must not be used or disclosed for a secondary purpose unless required by law or the individual consents to the use or disclosure.
3) Provider Independence.

The IVRP provider must not have a financial interest in the provider of the educational material. For example, if company A, the training materials provider, seeks services from company B, an IVRP provider, company B or its officers must not own shares in company A and there must be no common directors in either company. This is due to the potential degradation of the integrity of IVRP results (i.e.: the provider of training materials may have a financial incentive to minimize the impact of the IVRP so higher volumes of training materials can be delivered with less restrictions).

Note: Organizations using third-party ID verification and remote proctoring for the purpose of ensuring the privacy of training participants and to eliminate privacy infringement exposure should ensure that part of the process of vendor selection/award includes a privacy impact assessment and data security review.

[5] Information and Privacy Commissioner of Ontario, "Privacy by Design" by Ann Cavoukian, Ph.D., Information and Privacy Commissioner Ontario, Canada).

[6] Data Protection & Privacy 2014, Published by Law Business Research Ltd, London, UK, ISSN 2051-1280

5 Technological / Process Considerations and Best Practice

The goal of web-enabled IVRP is to eliminate hardware needs beyond those that are standard within computing devices such as microphones, speakers and video cameras. These enable the following to occur:

- Image and video capture
- Identity verification
- Confirmation of proctoring rules (e.g., detection of the presence of others in the immediate vicinity of the test participant)
- The use of facial recognition technology to confirm identity

Peripheral Devices

Additional peripheral devices, which monitor biometrics (fingerprint scanners, heartbeat monitors or retina scanners), can provide alternative methods of identity verification but are not widely available and as such not recommended.

The use of additional peripheral devises restricts usability amongst participant population and creates technological barriers that limit the ability of organizations to cost effectively ensure an adequate due diligence defence.

Invasive Software

The installation of software includes risks and limitations such as the transmission of viruses, software system requirements beyond the technical capability of the participant (e.g., employees do not have admin access permitting installation due to IT security architecture), upgrades required for new operating systems and potential limits on the data transfer allowance of the target computer. Web-enabled IVRP must be able to be activated from a web browser and not require any software installation (beyond browser/plugin updates) in order to operate.

Timeliness

Where identity verification and remote proctoring is not completed using, in some part, biometrics to make confirmations the turnaround time can be extensive and may not be appropriate to user and organizational needs.

Insecure Browser Detection

All users may be accessing the online training via any number of browsers. They may use computers and devices that are outside the control of their employer and as such there is no way of ensuring that they use secure browsers unless this control is integrated into the IVRP technology. An insecure browser jeopardizes the privacy of the information

transmitted when a user registers into the learning management system (LMS), submit a user/government photo and give access to their web-cam. As the security provided by the browser is based on it being up to date, the IVRP technology integrated into the LMS should check the browser version and restrict access to out-of-date browser access.

Live Monitoring

Where live monitoring is provided by a vendor special attention should be given to how the live proctoring impacts; the availability of services (due to scheduling requirements), evidence of infractions (if no recordings) and the consistency/accuracy of proctoring services (where multiple sessions are monitored simultaneously and thus divide the proctors' attention).

5.1 Accessibility Considerations and Best Practices

IVRP must be accessible:

1) On both internal networks and externally on the internet to allow for the delivery of training materials without limit to geographical location as long as an internet connection is present.
2) On multiple browsers, specifically internet Explorer, Firefox, Safari and Chrome is also required.
3) By third-party Educational Material providers for on-line offerings of Training materials and within Learning Management Systems.

Data Management

Data must be protected:

1) Via Password. Passwords must be one-way encrypted and not be accessible to anyone, even the developers.
2) During transfer. Data must be transmitted/received using a 256-bit security certificate - the standard in web security.
3) Physically. The data centre where the captured data is to be stored must be secure using features such as:

   ☐ Access key cards/biometric scanning

   ☐ 24/7/365 security guards

   ☐ SSAE 16 Certification

   ☐ Dual interlocking door + tailgate-proof mantrap

6 Adherence to Standard

As the intent of this guide is to protect the health and safety of workers as well as to assist employers wanting to meet their legal and ethical obligations, it is necessary to include a recommendation to organizations operating outside of the recommendations contained within this standard.

If an organization is not adhering to the expectations outlined within this document yet using training for the purposes of regulatory compliance, due diligence or as part of risk mitigation efforts, the method of training delivery should be restricted to instructor-led.

Although instructor-led training is a distinctly different method of training delivery, an organization should establish standards that clearly communicate their expectations as to how worker identity and participation is to be managed in the classroom. Not ensuring the integrity of training, no matter the method of delivery, creates the potential for the training to become purely 'administrative' and lose its risk mitigative value.

The integrity of training outside of the scope of this document i.e. training not part of regulatory, safety or due diligence requirements is purposely not discussed and should be based on organizational standards.

7 References

1) R. v. Bata Industries Ltd. (1992), 7 C.E.L.R. (N.S.) 245, 9 O.R. (3d) 329, 70 C.C.C. (3d) 394 (Prov. Div.)
2) R. v. Commander Business Furniture Inc. (1992), C.E.L.R. (N.S.) 185 (Ont. C.J.)
3) R. v. Rose's Well Services Ltd. (Dial Oilfield Services), 2009 ABQB 266
4) Getting the Deal Through, Data Protection & Privacy in 26 Jurisdictions Worldwide, 2014, Contributing editor: Rosemary P Jay.
5) Information and Privacy Commissioner of Ontario, "Privacy by Design" by Ann Cavoukian, Ph.D., Information and Privacy Commissioner Ontario, Canada).
6) Data Protection & Privacy 2014, Published by Law Business Research Ltd, London, UK, ISSN 2051-1280

Appendix A. IVRP Application Checklist

A.1. Privacy

- ☐ Data Segregation: Information e.g. media images, government ID should not be collected by or accessible to an entity that has other personal information on the individual e.g. Address, date of birth, age, gender
- ☐ Data Access: All media should be kept inaccessible to the employer, employer associations and agents if not required to demonstrate their identity to document non-compliance.
- ☐ Data Retention: All media should be deleted within twenty-four hours of collection if not required to demonstrate their identity or to document non-compliance.
- ☐ User Acknowledgement: The privacy policy and instructions must be presented, where reasonable, in a language understood by the user.
- ☐ Data use: The information e.g. must not be used or disclosed for a secondary purpose unless required by law or the individual consents to the use or disclosure

A.2. Technology

- ☐ Technology Availability/Acceptance: The IVRP method does not require additional peripheral devises (beyond the standard microphones, speakers and video cameras) that may create technological barriers.
- ☐ Invasive Software: Technology can be accessed through a web browser and does not require any software installation (beyond browser updates) in order to operate.
- ☐ Usability: Technology uses biometrics to identify users for ID comparison, to minimize ID requests for returning users and to validate user during proctoring.

A.3. Accessibility

- ☐ IVRP must be accessible across all standards-compliant browsers, such as Internet Explorer, Firefox, Safari, Opera, and Chrome
- ☐ IVRP must not be restrictive to LMS or course architecture i.e. functions with SCORM, flash, HTML and iframe training instructional as well as examination content

A.4. Security

- ☐ Data Integrity: The IVRP provider must not have a financial interest in the provision of the educational material or whether the users training is determined to be valid or in-valid based on IVRP findings.

- Browser: Technology identifies the browser type of the user and ensures that the browser is secure i.e., is a version still receiving security updates from its developer
- Data access: All passwords must be one-way encrypted and not be accessible to anyone, even the developers.
- Data transfer: Data must be transferred using at least a 256-bit security certificate
- Servers: The data centre where the captured data is to be stored must be secure using
- Access key cards/biometric scanning, 24/7/365 security guards, SSAE 16 Certification and dual interlocking door + tailgate-proof mantrap capabilities or alternative offering a higher degree of protection