



## **IOSH ALBERTA ASSOCIATION**

Industrial Occupational Safety & Health Association of Alberta

## **INDUSTRY BEST PRACTICE**

### **Web-Based Training Identity Verification and Proctoring**



IOSH Alberta Association  
Industry Best Practice | WTIVP-09092015V2

September 9, 2015

# Web-Based Training Identity Verification and Proctoring

## INDUSTRY BEST PRACTICE

Approved September 9, 2015  
Industrial Occupational Safety and Health Association of Alberta

IOSH Alberta Association

### **Abstract**

This Industry Best Practice has been developed based on the input and collaboration of the contributors listed within this document and provides a framework for understanding, utilizing, scrutinizing and integrating of identity verification and proctoring (IVP) technology with web-based training (WBT). This Industry Best Practice provides some guidelines and possible approaches for an organization to consider. It can serve as a baseline for helping employers assess and address the risks associated with conducting web-based training for regulatory critical educational materials.

## NOTICE AND DISCLAIMER

IOSH Alberta Industry Best Practices, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While IOSH Alberta administers the process it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its publications.

IOSH Alberta is an industry association with no regulatory, licensing or enforcement power over its members or anyone else. IOSH Alberta does not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines. It assumes no duty of care to the general public, because its works are not obligatory and because it does not monitor the use of them.

IOSH Alberta disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. IOSH Alberta disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person's or entity's particular purposes or needs. IOSH Alberta does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, IOSH Alberta is not undertaking to render professional or other services for or on behalf of any person or entity, nor is IOSH Alberta undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information covered by this publication may be available from other sources, which the user should consult for additional views or information not covered by this publication.

IOSH Alberta has no power, nor does it undertake to police or enforce compliance with the contents of this document. IOSH Alberta does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes best practices to be used as guidelines that third parties may or may not choose to adopt, modify or reject. Any certification or other statement of compliance with any information in this document should not be attributable to IOSH Alberta and is solely the responsibility of the certifier or maker of the statement.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of the copyright owner.

## **FOREWORD**

### **About IOSH Alberta Association**

The Industrial Occupational Safety and Health Alberta Association (IOSH Alberta) is an industry organization comprised of regional and multinational organizations operating mines, refineries, upgraders, pipelines, and chemical processing/manufacturing facilities, as well as providing operational essential services that include, but are not limited to, craning, heavy hauling, industrial cleaning, safety services, scaffolding and transport.

### **Association Objectives**

The objectives of the Association shall be collectively improving the workplace environment by updating Safety Standards and Loss Control practices by:

1. Promoting the improvement of occupational health and safety programs initiatives through collective sharing of information, experiences, programs and training.
2. Interacting with and supporting other councils in the influencing of legislative bodies in the formulation and application of Occupational Health and Safety legislation.
3. Establishing channels of communication with Safety Professionals, Government Agencies, Member Company Senior Management, other Safety Associations and the public when assistance or guidance is needed.
4. Providing recognition to Member Companies for outstanding Safety Achievements on an annual basis.

IOSH Alberta Association  
**Industry Best Practice | Web-Based Training Identity Verification and Proctoring**

---

**Working Group Members** (Below is a list of the IOSH Alberta Association members, participating industry representatives and key individuals providing subject matter expertise. Please note that participation by an individual does not necessarily indicate an organization's position with regards to this Best Practice).

**AGRA Foundations** (Drago Ranisavljevic)  
**Agrium Inc.** (Cory Wald | Mark Ropchan)  
**ALE Roll-Lift Canada** (Charles Lott | Bas Bronder)  
**Aluma Systems** (Ben Bunce)  
**Brock Canada Inc.** (Stephen McAllister)  
**Canadian Industrial & Construction Training CICT** (Jane Glavine | Dave McDonald)  
**CEDA** (Tamara Kapanen | Craig Nicholson)  
**Century Wireline Services** (Sasha Laczko | Robert Racz)  
**Chemco Electrical Contractors** (Matthew Hofer)  
**Clean Harbors** (Donald Adams | Ron Ovenden)  
**Comco Pipe & Supply** (Zack Deis | Kevin Stack)  
**Decca Consulting Inc.** (Leigh-Anne Hicks | Marlaina Huery)  
**Dow Chemical** (Bryan Conroy | Riaz Usman | Justin Skopyk)  
**Edcon Power Tongs & Oilfield Services Ltd.** (Lorne Halisky)  
**Edmonton Exchanger & Refinery Services** (Michael Spring)  
**Geopac Inc.** (Amanda Mahoney)  
**Husky Energy** (Lorne Halisky)  
**Imperial Oil (Strathcona Refinery)** (Lawrence Craig)  
**KBL Environmental Ltd.** (Jeff Dirks)  
**Mammoet Canada Western Ltd.** (Sheldon Redpath | Wim Van Beek)  
**Mattawa Industrial Inc.** (Hayley Whitlock)  
**McLennan Ross** (David Myrol) **Subject Matter Expertise**  
**MEGlobal Canada** (Rob Jost | Al Rowley | Dale Sandford)  
**Oerlikon Metco** (Gerry Mason)  
**Occupational Health & Safety** (Gerry Wagner | Alex Gomez)  
**Owens-Corning Canada** (Kevin Roblin)  
**Quadra Industrial Services Ltd.** (Gillian Bowering)  
**SPI Health and Safety** (Chad Morin | Murray Oleksyn)  
**Safety Direct Ltd.** (Marc Scuccato | Brett Zeissler)  
**Safway Services Canada Inc.** (Bryan Getson)  
**Sarens Canada Inc.** (Alyssa Espenant | Shawna Boreen)  
**Shell Canada Energy** (Duane Seelochan)  
**Sherritt International Corporation** (Brenda Bakke | Sandi Miller)  
**Standard Scaffold & Insulation Inc.** (Whitney Allen | Dan McLeod)  
**Sterling Crane** (Russ Brown)  
**Suncor (Edmonton Refinery)** (Martin Mudryk)  
**Tool Safe Products Ltd.** (Cheryl Ann-Orr)  
**Umicore Canada Inc.** (Wendy Lyka)  
**United Rentals** (Ryan Heinish)  
**United Safety Ltd.** (Justin Pellerin)

**Western Safety Consulting Inc.** (Dave Hasson | Russell MaKar | Chris Campbell | Alex Paredes)

**Windsor Salt (The Canadian Salt Co. Ltd.)** (Cameron Kirkpatrick)

**Workers' Compensation Board** (Boris Makale)

**Zep Manufacturing Inc.** (Carlos Pereira | Ron Lehmann)

## TABLE OF CONTENTS

<b>1.0</b>	<b>Introduction .....</b>	<b>08</b>
<b>2.0</b>	<b>Definitions.....</b>	<b>09</b>
<b>3.0</b>	<b>Standard.....</b>	<b>10</b>
3.1	Use of Web-enabled Identity Verification and/or Proctoring (IVP) .....	10
	a) Rationale for the use of Web-enabled Identity Verification, Proctoring or Both .....	10
3.2	Legal Considerations .....	11
	a) Legal Disclaimer .....	11
	b) Due Diligence Defence .....	11
	c) Paramountcy of Engineering Controls.....	11
	d) Privacy.....	12
	e) Provider Independence .....	12
	f) Case Commentary .....	12
3.3	Technological Considerations .....	13
	a) Software .....	13
	b) Hardware.....	13
	c) Accessibility.....	13
	d) Data Management.....	14
<b>4.0</b>	<b>References .....</b>	<b>15</b>

## Figures

1)	Utilization Rationale .....	10
----	-----------------------------	----

## **1.0 Introduction**

An inherent challenge associated with the delivery of educational materials and their associated comprehension verification activities (tests, demonstrations, etc.) is the potential for participants to act dishonestly or unfairly in order to gain an advantage during an examination, commonly referred to as “cheating”.

This naturally leads to the need for instructors to verify the identity of participants and for a supervisor or proctor to monitor the taking of examinations to ensure both the rules of the examination are followed and the identity of each participant is verified.

The advent of the internet provided the opportunity to facilitate the delivery of web-enabled educational materials. This was quickly seized upon by organizations across the globe, yet the corresponding activities of identity verification and proctoring of training or examinations was not commonly integrated.

Fortunately, web-enabled identity verification and proctoring (IVP) have become more available and reduced in cost to a point where widespread application of this technology is now possible. IVP technology is particularly critical when organizations use web-enabled educational materials as part of risk control strategies that seek to ensure that 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).

In order to ensure that IVP sufficiently meet requirements to safeguard the integrity of educational material delivery and the integrity of a resulting due diligence defence (in the case of health, safety and environment domain), this standard has been developed to provide organizations with the information needed to ensure the methodology and technology chosen to administer IVP meets organizational needs and legal requirements.



## 2.0 Definitions

**Due Diligence Defence** is a legal defence available to an organization 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 facial characteristics of the individual in a digital image compared with a credible form of photographic identification also presented in a digital image.

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

**Proctoring** is the use of web-enabled technology to supervise an examination or delivery of educational materials.

**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.

**Randomized Proctoring** is the use of a statistically based algorithm to trigger the proctoring of a pre-determined percentage of sessions, stated in this paper as no less than 10% of all sessions.

**Regulatory Critical Educational 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.

### 3.0 Standard

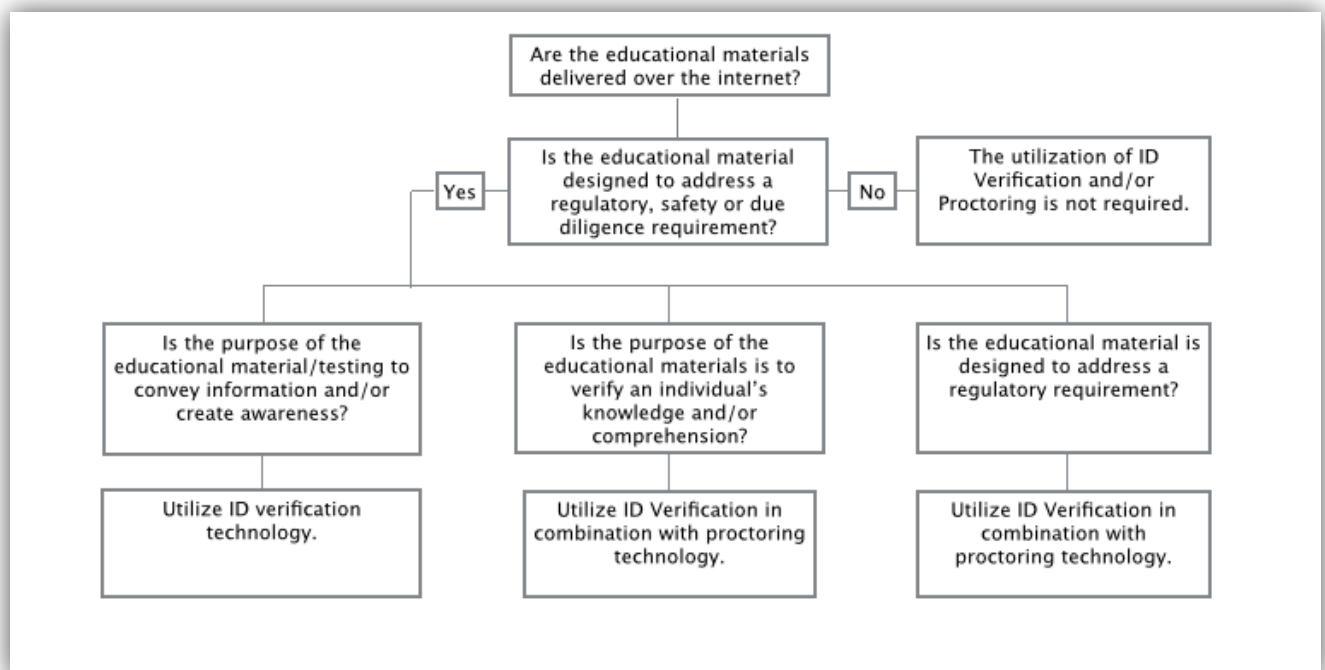
#### 3.1 Use of Web-enabled Electronic Identity Verification and/or Proctoring (IVP)

- a) Rationale for the use of Web-enabled Identity Verification, Proctoring or Both

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. Proof of competency 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 1.0 below leads one through making the decision of when and what aspects of the technology to use.

Figure 1.0 – Utilization Rationale



### **3.2 Legal Considerations**

#### a) 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.

#### b) 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. If the organization fails to discharge its burden of proof, then a conviction will result. Although the system is subject to technological limitations, given advances in internet technology, the benchmark for technological limitations in relation to web-enabled IVP 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 IVP economical and reliable, such systems should be incorporated into the delivery of, and associated examinations for, web-enabled educational materials.

#### c) 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. 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.

d) Privacy

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 (reference: *Data Protection & Privacy 2014, Published by Law Business Research Ltd, London, UK, ISSN 2051-1280*).

Additional privacy requirements for web-enabled IVP should include:

- i) The requirement that proof of identity and/or violations and must be held external to the provider of educational materials and only released to the utilizing organization where legally required.
- ii) Persons subject to IVP must be provided with the privacy policy and instructions for use in a language they understand.
- iii) 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.

e) Provider Independence

The IVP provider must not have a financial interest in the provider of the educational material. For example, if company A, the educational materials provider, seeks services from company B, an IVP 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 IVP results (i.e.: the provider of educational materials may have a financial incentive to minimize the impact of the IVP so higher volumes of educational materials can be delivered with less restrictions).

f) Case Commentary

The Alberta case of *R. v. Rose's Well Services Ltd.* provides an example of both the identity verification problem and 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 Enform (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 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.

### **3.3 Technological Considerations**

#### **a) 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 IVP must be able to be activated from a web browser and not require any software installation (beyond web browser installation) in order to operate.

#### **b) Hardware**

The goal of web-enabled IVP 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); and
- The use of facial recognition technology to confirm identity.

Additional peripheral devices, which monitor biometrics (fingerprint scanners, heartbeat monitors or retina scanners), are not widely available and are not recommended.

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

#### **c) Accessibility**

IVP must be accessible:

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

d) Data Management

Data must be protected:

- i) Via Password. Passwords must be one-way encrypted and not be accessible to anyone, even the developers.
- ii) During transfer. Data must be transmitted/received using a 256-bit security certificate - the standard in web security.
- iii) Physically. The data centre where the captured data is to be stored must be secure using features such as:
  - a. Access key cards/biometric scanning
  - b. 24/7/365 security guards
  - c. SSAE 16 Certification
  - d. Dual interlocking door + tailgate-proof mantrap

#### **4.0 References**

1. *Getting the Deal Through, Data Protection & Privacy in 26 Jurisdictions Worldwide, 2014, Contributing editor: Rosemary P Jay.*
2. *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.)*
3. *R. v. Commander Business Furniture Inc. (1992), C.E.L.R. (N.S.) 185 (Ont. C.J.)*
4. *Data Protection & Privacy 2014, Published by Law Business Research Ltd, London, UK, ISSN 2051-1280*