OHIO DEPARTMENT OF PUBLIC SAFETY

ONLINE DRIVER EDUCATION SECURITY ASSESSMENT

The Ohio Department of Public Safety (ODPS) recommends that any online provider adhere to the Center for Internet Security (CIS)[1], ODPS' minimum technical requirements for online driver education providers are listed below.

ODPS requests that online providers provide detailed explanations regarding how the providers are meeting each of the outlined requirements. Please be aware that incomplete or insufficient responses may result in a follow-up discussion with an ODPS IT Security Consultant in order to clarify security assessment responses, if necessary.

For the purpose of this assessment, the definition of personal information is aligned with **Ohio Revised Code (R.C) 4501:1-20-02 Driver's privacy protection (A)(1)**.[2]

> *"Personal information" means information contained in a motor vehicle record that identifies an individual person, including but not limited to, the person's photograph, digital image, digitalized photograph, social security number, driver or driver's license identification number, name, date of birth, telephone number, medical or disability information, or a person's address other than the county and five-digit zip code. "Personal information" does not include information pertaining to a vehicular accident, driving or traffic violation, or driver's status, or a name that is provided by the requester.*

Please enter the URL of the login page for your Online Driver Education program here:

1. INVENTORY AND CONTROL OF ENTERPRISE ASSETS

Providers shall actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

- Provider shall describe how they actively manage and track the enterprise assets.
- Provider shall describe how they monitor and identify unauthorized assets in order to remediate or remove them from the network.

[1] The 18 CIS Critical Security Controls (cisecurity.org)

[2] See http://codes.ohio.gov/oac/4501%3A1-12-02 for additional details.

2. INVENTORY AND CONTROL OF SOFTWARE ASSETS

Provider shall actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

- Provider shall describe how they actively manage and track all software.
- Provider shall describe how they monitor and identify unauthorized software to prevent it from installation or execution.

3. DATA PROTECTION

Providers shall develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Explain how the provider currently meets these requirements.

4. SECURE CONFIGURATION OF ENTERPRISE ASSETS AND SOFTWARE

Providers shall establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
Provider shall apply most current security patches to the operating system, installed software packages, databases, and web servers.

Explain how the provider currently meets these requirements.

ACCOUNT MANAGEMENT

Provider shall use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.
In addition, system users shall be logged off after a standard period of inactivity, including the following:

- At a maximum, external (student) and internal (employee) users shall be logged off after thirty (30) minutes of inactivity.
- At a maximum, all user accounts shall be disabled after a period of sixty (60) days of inactivity.

Explain how the provider currently meets these requirements.

5. ACCESS CONTROL MANAGEMENT

Provider shall use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software. This includes, at a minimum:

- Complex passwords;
- Scheduled change of passwords for each user at an interval of no longer than six months;
- Documented procedures for requesting, granting, removing, and reviewing administrative account privileges;
- Utilization of access control of accounts to ensure administrative accounts are used for administrative purposes only.

Security personnel must be notified within 24 hours of the addition of an account with administrative privileges. Every 24 hours after, the system must alert or send an email about the status of the administrative privileges until the unauthorized change has been corrected or authorized through a change management process.

Explain how the provider currently meets these requirements.

6. CONTINUOUS VULNERABILITY MANAGEMENT

Provider shall develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Explain how the provider currently meets these requirements.

7. AUDIT LOG MANAGEMENT

Provider shall collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack. Provider must be capable of logging all events. Logging of events shall include date, timestamp, source address, destination address, and other details about the packet. When a device detects that is not capable of generating logs (due to a server crash or other issue), it shall generate an alert or email notification for enterprise administrative personnel within 24 hours.
Providers shall conduct recurring comprehensive security audits that, at a minimum, include running reports to identify anomalies and documenting findings and steps taken to mitigate any identified deficiencies.

Explain how the provider currently meets these requirements.

8. E-MAIL AND WEB BROWSER PROTECTIONS

Provider shall improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Explain how the provider currently meets these requirements.

9. MALWARE DEFENSES

Provide shall prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
Explain how the provider currently meets these requirements.

10. DATA RECOVERY

Provider shall establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

- Providers shall maintain and document Data recovery & Business Continuity plans and be able to furnish documentation upon request.

Explain how the provider currently meets these requirements.

11. DATA PROTECTION

Providers shall handle, store, and process confidential personal information (CPI)[3] or other information that is required to be protected by law, regulation, or executive order, in an encrypted format. Providers shall monitor for and alert unauthorized attempts to access and / or transmit CPI. The relevant security system(s) shall identify and alert the provider of unauthorized data extraction within one hour of the occurrence. Upon detection of unauthorized access or attempted access, the system shall notify the provider every twenty-four (24) hours until the source of the event is identified and the risk is mitigated.

Explain how the provider currently meets these requirements.

12. COMPLIANCE WITH SECURITY AND PRIVACY REGULATIONS

Providers shall be reasonably aware of relevant security and privacy regulations. Specifically, providers shall comply with iNACOL Course Standards 2011[4], with Section A (Content), Item 11 (privacy policies) and Section D (Technology), Item 11 (confidentiality controls).

> ***A11 – Privacy policies are clearly stated****. A policy statement is posted on the course provider's website and in the course and is easily found by the student. The policy discloses the organization's information gathering and dissemination practices.*
>
> ***D11 – Student information remains confidential, as required by the family Educational Rights and Privacy Act (fERPA)****. Defined course procedures for reporting grade and student information comply with the family Educational Rights and Privacy Act (fERPA).*

Providers shall also implement reasonable security measures to validate the identity of the student and the student's parent prior to granting the student access to the training system.

Explain how the provider currently meets these requirements.

Certification Statement: I hereby certify I am the authorizing official of this online driver education program and the information contained herein is true and accurate. I have read, understand, am familiar with, and am responsible for knowing and understanding the security provisions governing online schools and online instruction as those provisions are set forth in Chapter 4508. of the R.C. and Chapter 4501-7 of the Administrative Code, which incorporates this security assessment. I further understand that a false statement on this document constitutes falsification under section 2921.13 of the R.C., which is a first degree misdemeanor, and may also result in the denial, suspension, or revocation of my online provider license.

To all herein I so certify and attest with my signature below.

SIGNATURE OF THE AUTHORIZING OFFICIAL	DATE OF SIGNATURE
X	

[3] http://codes.ohio.gov/oac/1301-1-03

[4] http://www.inacol.org/cms/wp-content/uploads/2013/02/iNACOL_CourseStandards_2011.pdf

STATE OF OHIO
COUNTY OF _____

The foregoing instrument was acknowledged before me this _____ day of _____ ,20 _____ ,

by _____ .
NAME OF PERSON ACKNOWLEDGED

X _____
NOTARY PUBLIC

My commission expires _____ ,20 _____

_____
PRINTED NAME