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 National Institute of Standards and Technology (NIST) information security standards[1], and the SANS Institute's 20 Critical Security Controls[2]. However, 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)**.[3]

> *"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. HARDWARE, SOFTWARE, AND INTERNET CONNECTION SPEED

List the hardware, including the make, model and operating system version and software with version information that will be used by the provider to administer the online driver training. Make sure to include all web, database, file, and application servers that store and / or transmit training application data. Additionally, please specify the Internet connection speed that will be used by the provider to administer the online training.

[1] Specifically, Special Publication 800-53, Rev 3: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf and Special Publication 800-30, Rev 1: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[2] http://www.sans.org/critical-security-controls/guidelines.php

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

2. RISK MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY

Online providers shall have in place Risk Management, Business Continuity, and Disaster Recovery plans. Describe those plans utilized by the provider. Please include relevant information regarding offsite storage and processing facilities, facilities used in the event that a disaster damages or destroys your primary data processing facility.

3. SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS, AND SERVERS

Providers shall apply standard secure configurations for the operating system as recommended by the operating system provider before releasing those systems to production. Providers shall apply security patches to the operating system, installed software packages (Adobe, Java, etc.), databases, and web servers.

Explain how the provider currently meets these requirements.

4. MALWARE DEFENSES

Providers shall employ automated anti-malware and anti-virus software on all workstations, servers, and mobile devices to ensure the most up-to-date version(s) is used. Systems must block installation, prevent installation, or quarantine malicious software within one hour, alerting or sending an e-mail when this action has occurred.

For the purposes of this control, mobile devices do not include smartphones. However, providers are strongly encouraged to evaluate the need for anti-malware technologies for smartphones and other handheld devices to the extent that they are in use within the scope of the enterprise.

Explain how the provider currently meets these requirements.

5. APPLICATION SOFTWARE SECURITY

Providers shall utilize a web application security controls (web application vulnerability scans, web application firewalls, etc.) to protect against unauthorized access and attacks. Security monitoring systems shall scan all Internet-accessible web applications on a regular basis and shall, at a minimum, generate an alert or send an e-mail to the enterprise administrative personnel within 24 hours of a detected attack. Should a scan fail to be successfully completed, the security system must alert or e-mail the administrative personnel within one hour indicating the scan was unsuccessful. All Internet-accessible web applications identified shall be fixed (or a compensating control implemented) within 15 days of the discovery.

Specify the specific firewall used and response to alerts that comply with these requirements.

6. WIRELESS DEVICE CONTROL

If the provider uses wireless technology within their office network, they must secure the wireless connections with at least standard management tools that, at a minimum, run commercial wireless scanning, detection, discovery tools, and wireless intrusion detection systems. The system must be capable of identifying unauthorized wireless devices or configurations when they are within range of the provider's systems or connected to their networks. The system must be capable of identifying any new unauthorized wireless devices that associate or join the network within one hour, alerting or sending e-mail notification to a list of enterprise personnel. The system must automatically isolate an attached wireless access point from the network within one hour and alert or send e-mail notification when isolation is achieved. The system must be capable of identifying the location, department, and other details of where authorized and unauthorized wireless devices are connected to the network. In lieu of an automated wireless intrusion detection system, a documented manual process may be considered an acceptable alternative.

Explain how the provider currently meets these requirements.

7. DATA RECOVERY CAPABILITY

At a minimum, critical application data shall be backed up daily. At a minimum, providers shall perform a monthly integrity test to ensure data can be successfully restored from backups. If backup data is stored on media (i.e. hard drives and tapes, etc.), that media shall be secured in a locked facility, preferably off-site.

Explain the backup strategy and the security measures for the backup data used by the provider to meet these requirements.

8. SECURE CONFIGURATIONS FOR NETWORK DEVICES SUCH AS FIREWALLS, ROUTERS AND SWITCHES

Providers must have documented standard secure configurations for all network devices deployed within the business. To ensure that system or application software is kept current, any unused or unnecessary software shall be uninstalled and removed from the provider's system within 24 hours of its discovery. The system must be capable of identifying any changes, including modifications to key files, services, ports, configuration files, or any software installed on the device. Modifications include deletions, changes, or additions of new software to any part of the device configuration. The configuration must be checked against the master image database to verify any changes to secure configurations that would impact security. This includes both the operating system and configuration files. Any of these changes to a device or operating system must be detected within 24 hours and notification sent to a list of enterprise personnel. The system must send notification about the status of the system until the change(s) have been investigated and remedied.

Explain how the provider currently meets these requirements.

9. CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

Providers must have controls around administrative privileges within the provider's systems that, at a minimum, provide for the following:

- Complex passwords (letters, numbers, special characters);
- 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 via an alert or e-mail within 24 hours of the addition of an account with administrative privileges. Every 24 hours after that point, the system must alert or send e-mail about the status of the administrative privileges until the unauthorized change has been corrected or authorized through a change management process.

Explain the tracking and limitations the provider currently uses to meet these requirements.

10. MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS

The system must be capable of logging all events across the network. The logging must be validated across both network-based and host-based systems. Any logged event must generate a log entry that includes the date, timestamp, source address, destination address, and other details about the packet. Any activity performed on the network must be logged immediately to all devices along the critical path. When a device detects that it is not capable of generating logs (due to a server crash or other issue), it shall generate an alert or e-mail notification for enterprise administrative personnel within 24 hours.

- Providers shall store audit logs for the user activity for three (3) years from the date of completion of the activity and review them annually for discrepancies.
- 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.

11. ACCOUNT MONITORING AND CONTROL

Providers must have controls to monitor and control systems and user accounts. The system must be capable of tracking and disabling accounts. System users shall be logged off after a standard period of inactivity.

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

Explain the controls used by the provider for these requirements.

12. DATA PROTECTION

Providers shall handle, store, and process confidential personal information (CPI)[4] 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.

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

13. 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[5], 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	

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

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