IN THE SUPREME COURT OF THE STATE OF ARIZONA
ADMINISTRATIVE OFFICE OF THE COURTS

In the Matter of:	)	
	)	
ARIZONA CODE OF JUDICIAL	)	Administrative Directive
ADMINISTRATION § 7-205	)	No. 2018 - 11
IT STANDARDS FOR	)	
DEFENSIVE DRIVING SCHOOLS	)	
	)	

On May 2, 2018, Administrative Order No. 2018-38, amending ACJA § 7-205: Defensive Driving was issued. As amended, ACJA § 7-205 provides the Director of the Administrative Office of the Courts (AOC) authority to establish IT standards.

The purpose of this directive is to establish IT security requirements for all certified defensive driving schools. The AOC developed draft standards and provided the standards to the schools for comment. After consideration of school comments, the AOC developed the standards attached as Exhibit A ("IT Standards"). Therefore,

IT IS DIRECTED that pursuant to ACJA § 7-205 (E)(1)(v), the IT Standards are adopted as the minimum standards required of all certified defensive driving schools.

IT IS FURTHER DIRECTED that all schools shall implement the IT Standards on or before January 15, 2019:

Dated this 26th day of November, 2018.

DAVID K. BYERS
Administrative Director of the Courts

EXHIBIT A

Arizona Judicial Branch Minimum Security Standards for Defensive Driving Schools

State law and state policy require government entities, including court vendors, to protect certain personal information collected in the course of conducting business and providing services. The following standards are necessary in furtherance of the intent of these laws.

A. Defensive Driving Schools Storing Any Specified Data Elements Defined in A.R.S. §18-551(11)

Follow controls specified in NIST SP 800-171 for access, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, and information integrity, at a minimum. ISO 27001 controls may be employed instead. Provide third-party certification of compliance with either standard at the frequency specified by the AOC*.

Maintain or ensure the payment processing provider maintains all credit card data in compliance with the current release of the Payment Card Industry Data Security Standard and submit the most recent proof of compliance to the AOC when requested. AOC will maintain compliance information received as confidential.

Maintain a formal, written policy for protection of confidential personal information and notification of affected persons in the event of a breach that exposes unencrypted or unredacted personal information not otherwise publicly available, as required in A.R.S. §18-551.

* Certification of compliance by the vendor supplying cloud-hosted services to the school is also acceptable.

B. Schools Accessing AOC Data <u>But Not</u> Storing Any Data Elements Defined in A.R.S. §18-551(11)

ID #	Minimum Requirements or Control
	1. System Protections
1.1	Individual UserIDs all conform to a standard format. Guest and generic UserIDs should be disabled.
1.2	User IDs are deactivated after a 30-day period of inactivity. IDs are reviewed for deletion after 60 days. Deactivation or deletion may be extended by written management approval.
1.3	Passwords have a minimum length of 8 characters with complexity enforced to include upper case, lower case, and numbers.
1.4	Every user ID has a password conforming to 1.3. Passwords are changed at least once every 90 days.
1.5	Every password on a system is changed at the time of the next log-in whenever that system's security has been compromised or there is a convincing reason to believe it has been compromised.

ID #	Minimum Requirements or Control
1.6	Whenever an employee is terminated, his or her user access is promptly revoked.
1.7	Termination of an employee with "Admin" system access results in immediate password change to all systems.
	2. Data Protections
2.1	All server and client devices accessing the school network have up-to-date anti-virus protection on them. Anti-virus programs are protected against user access and never disabled.
2.2	All servers and workstations have approved anti-virus screening software enabled on their computers at all times. Users can not disable or deactivate this software.
2.3	All "private " or "confidential personal information" as defined in A.R.S. §18-551 transmitted in digital format is only communicated in encrypted form.
2.4	All downloaded files are screened with virus detection software prior to being opened/saved/ executed.
2.5	All devices that access court information employ a locking screen saver program which requires a password to access. Timeout is set to no longer than 15 minutes of inactivity for any public accessible device, including all laptops; 60 minutes for devices within any locked area by approval of school management.
2.6	All computer and network devices are maintained with the latest vendor-provided security updates available for the specific operating system.
2.7	Security audit scans of all computing devices occur not less than twice per year. Any vulnerabilities identified must be remediated prior to accessing the court network. AOC may request scan results and will maintain such information as confidential.
2.8	All local applications loaded on desktop/laptop systems are patched to prevent known/reported/ patchable security vulnerabilities.
2.9	Data capturing tools are prohibited on the court network.
2.10	All credit card data shall be maintained in compliance with the current release of the Payment Card Industry Data Security Standard. AOC may request the most recent audit results and will maintain such information as confidential.
2.11	Maintenance of a formal, written policy for protection of confidential personal information and notification of affected persons in the event of a breach that exposes unencrypted or unredacted personal information not otherwise publicly available. (A.R.S. 18-551)

[Link to A.R.S. §18-551 at ww.azleg.gov once published]