**Section 176.240 Notary Public Course of Study − Provider Website and Security Requirements**

a) Each provider’s website must display the following information on its homepage:

1) the provider’s Secretary of State certification number; and

2) a statement that complaints regarding the provider may be directed to the Secretary of State’s Index Department. Contact information for the Index Department must be included with the statement.

b) A provider offering an online course must offer the course from a single domain. The course may accept students that are redirected to the online course domain, as long as the provider’s certification number appears on the source that redirects the students to the online course domain. The student must be redirected to a webpage that clearly identifies the certified provider offering the course before the student begins the registration process, supplies any information, or pays for the course.

c) A provider offering an online course may choose an existing webinar system or create its own webinar system.

d) Providers are prohibited from selling or disclosing any consumer information provided by the student unless the provider is disclosing the consumer information with a third party solely for the purpose of providing dynamic knowledge-based identity verification. The provider's contract with the student must clearly state whether the provider is disclosing consumer information for the purpose of providing dynamic knowledge-based identity verification. A statement concerning the prohibition on the sale or disclosure of student consumer information must be posted on the provider’s website in a conspicuous location.

e) Providers are prohibited from requesting the Social Security numbers of students, except for a request from a third-party process or service used by a provider to verify the identity of students taking a provider's course, in which case the third-party process or service must not share the Social Security number data with the provider.

f) Providers must take all necessary measures to prevent unauthorized access to consumer information, either in printed or electronic form. Upon discovery of a breach or unauthorized access, the provider must immediately report any unauthorized access to the Department.

g) Provider servers must be located in a secure location, with access restricted to only those employees or persons who have a business need to access the server.

h) Providers may use a third-party payment processing merchant for processing payments only if the provider’s contract clearly indicates to the student, before payment is made, the name of the third-party payment processing merchant to be used and the fee, if any, charged by the payment processor.

(Source: Added at 47 Ill. Reg. 8640, effective June 5, 2023)