Addendum: for use with Ohio Property & Casualty and Personal Lines online ExamFX courses and study guides version 24492en/24493en (P&C), and 24494en (PL) per exam content outline updates effective 07/01/2019.

*The following are **content additions** to supplement your existing text:*

Property and Casualty Insurance Basics

D. Ohio Laws, Regulations and Required Provisions

Fire Loss – Treasury Certificate

If fire damage to a structure located within a municipal corporation or township results in a recoverable amount higher than $5,000, the insurer must be furnished with a certificate from the county treasurer. Upon the written request from the insured specifying the tax description of the property and the receipt of proof of loss, the county treasurer will provide the insurance company with one of the following certificates:

A treasury certificate stating there are no delinquent taxes, assessments, penalties, or charges against the property; or

- A treasury certificate and bill showing the amounts of delinquent taxes, assessments, penalties, or charges against the property.
- If a bill is issued with the certificate, the insurer must pay the delinquent amounts with insurance proceeds, prior to paying the claim.

If a certificate is issued and there are no outstanding charges, the insurer may pay the claim associated with the damaged structure. If the agreed upon loss exceeds 60% of the aggregate limits of liability on the fire policy, the insurer must:

- Pay $2,000 for every $15,000 of the claim to a designated officer of the municipal corporation or township; or
- Pay the amount specified in a contractor's estimate to a designated officer of the municipal corporation or township.

If funds are determined to be in excess of the estimate and the municipal corporation or township has not incurred any costs as a result of repairs, removal, or securing, the funds will be returned to the named insurance within **60 days** of the designated officer receiving proof of completion.

If a building or other structure is insured through multiple companies, proceeds are paid on a **pro rata basis**.

3. Cancellation and Nonrenewal

Personal Policy Cancellation

If the cancellation of a personal lines insurance policy is for nonpayment of premium, a notice of cancellation must be mailed to the insured at least **10 days** prior to the cancellation. Notice of cancellation for nonpayment of premium may be included with a billing statement. Cancellation may occur on or after the due date of the bill, as long as the insured has been alerted in the required time frame.

Insurance Regulation

B. State Regulation

6. Insurance Information Privacy

Cyber Security

Cyberattacks are an alarming and ongoing threat, often resulting in the theft of sensitive consumer financial and health information, repair costs to hardware and software, litigation costs, and damage to a company's reputation. This has led to increasing calls for legislation and regulation for enhanced cybersecurity measures to address the numerous risks posed by a cyberattack.

An insurer's Information Security Program must be designed to do the following:

- Protect the security and confidentiality of nonpublic information and the security of the information system;
- Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;
- Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer; and
- Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

Training and Monitoring

As part of a cybersecurity program, insurers must designate one or more employees who are responsible for the information security program, as well as identify foreseeable internal or external threats that could result in an unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including information accessible to, or held by, third-party service providers. In addition, insurers must provide employee training and management, and implement safeguards to manage threats and assess the effectiveness of the safeguards' systems and procedures at least annually.

Insurers must submit a written statement to the Superintendent of Insurance by **February 15th** of each year, unless otherwise specified. The statement must certify that the insurer is in compliance with state cyber regulations.

Investigation of Events

In the event a cybersecurity event has occurred, a licensee, an insurer or third-party service provider must conduct a prompt investigation. This investigation must include:

- A determination whether a cybersecurity event has occurred;
- An assessment of the nature and scope of the cybersecurity event;
- Identification of nonpublic information involved; and
- Overseeing of reasonable measures to restore the security of the information system to prevent future cybersecurity events.

Licensees must maintain records concerning all cybersecurity events for a period of at least **5 years** from the date of the cybersecurity event and must produce those records upon demand of the Superintendent of Insurance.

Exemptions

The following are exempt from cybersecurity regulations:

- Insurers that have fewer than **20 employees**;
- Insurers with a gross annual income less than **$5,000,000**;
- Insurers with less than **$10,000,000** in assets at the end of the licensee's fiscal year; or
- Employees, agents, representatives, independent contractors, or designees of an insurer.

If a previously exempt insurer no longer qualifies for an exemption, the insurer may continue business without an Information Security Program for no more than 180 days. After this period has elapsed, the insurer must comply with state cyber requirements.

Definitions

Cybersecurity Event: any effort to obtain unauthorized access to an information system or nonpublic information stored on the information system. Cybersecurity events do not include instances in which acquired nonpublic information is returned, destroyed, or not used.

Encrypted: transformation of data to obscure meaning without the use of a protective process or key.

Information System: an organized system that collects, maintains, and transmits electronic nonpublic information.

Nonpublic Information: any business-related information that is not publicly available information that if misused could jeopardize a covered entity's security and operations; any personally identifiable information (such as social security number, driver's license, or credit card numbers); and any information (other than age and gender) related to health care.

Multi-Factor Authentication: authentication through verification of at least two factors:

- Knowledge factor, such as a password;
- Possession factors, such as a token or text message on a mobile phone; or
- Inherence factors, such as a biometric characteristic.

Publicly available information: information lawfully available to the general public from federal, state, or local government records, distributed media, or disclosures required by federal, state, or local law. Information may be considered publicly available if an insurer determines it's of the type available to the public and the consumer has not denied making it public.

Risk Assessment: evaluation of potential risks to the privacy of nonpublic information.

Third-party Service Provider: contracted person other than an insurer who is permitted to access nonpublic information for the purposes of maintaining, processing, or storing information.