VERMONT
DEPARTMENT OF FINANCIAL REGULATION
89 Main Street, Montpelier, VT 05620 - 3101
(p) 802-828-3304 | http://www.dfr.vermont.gov/

CAPTIVE INSURANCE DIVISION
CYBERSECURITY BEST PRACTICES

Preamble

A captive insurer and/or its parent organization should create an information security program that is commensurate with its size, complexity, and structure. The goal of the information security program should be to assess cyber risks and related controls in place to mitigate those risks and to develop a response plan should a cybersecurity event occur. Regular risk assessments can help prevent breaches. Factors that influence exposure include the type of data held/sensitivity of data, vendor access to data (the more people who can access the system, the higher the risk), the number of records, the complexity of the IT environment and the number of systems that "talk to each other".

A cybersecurity event means an event resulting in unauthorized access to, disruption or misuse of, an information system or information stored on such system. A cybersecurity event does not include: 1) the unauthorized acquisition of encrypted information if the encryption, process or key is not also acquired, released or used without authorization, 2) an event in which the organization has determined that the information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

Risk Assessment

- The organization should assess the sensitivity of the information it holds (i.e., proprietary business information, HIPAA protected information, personal identifiable information etc.) and weigh its retention policies against the business value.
- The organization should assess where sensitive data is stored, including sensitive data stored with third party service providers.
- The organization should attempt to identify internal and external threats that could result in unauthorized access of information, the dissemination of private information, and the destruction of critical information. This assessment should include an inventory of assets and device management and a list of service providers that have access to or hold sensitive information.

Risk Management

- The organization should engage employees in training on cybersecurity.
- The organization should have access controls on systems to ensure that only authorized users have access, this access should be audited regularly to ensure that each user still requires access to execute its duties.

- The organization should restrict physical access to facilities in the same way it restricts digital access to systems.
- All nonpublic information should be encrypted in transmission.
- The organization should implement multi-factor authentication to access systems in addition to passwords.
- The organization should periodically conduct penetration testing and vulnerability assessments.
- The organization should regularly test backup solutions to ensure that disaster recovery plans can be executed in a timely and effective manner. There should be a plan in place for damage due to environmental hazards such as fire or water damage or other catastrophes (earthquake, hurricane, etc.).
- The organization should evaluate the adequacy of cybersecurity practices of third-party service providers that have access to or hold sensitive information, including policies for access controls (multi-factor authentication), encryption, and notice to be provided to the organization in the event of incident involving its information.
- The organization should conduct periodic assessments of service providers based on the risk(s) they present and consider obtaining written representation to address the service provider's cybersecurity policies and procedures.
- The organization should have in place an oversight committee or CIO to ensure the information security plan is up to date and maintained.

Investigation of Cybersecurity Events

As part of its information security program, an organization should have a written plan in place for how to respond to cyber incidents. This should address the following:

- The internal process for responding to a cyber incident, including clear roles, responsibilities, and decision-making authority – designating specific individuals for each task.
- Designate who will investigate the incident to determine nature and scope.
- Process for sharing information both internally (employees) and externally (law enforcement, regulators). This should include a list of all regulatory bodies that should be notified with any required timelines.
- Plans for the identification of any potential weak points and how to mitigate them to ensure that the cyber event does not occur again.

Notification of Cyber Incident

After a cyber incident has occurred the organization must report it to the relevant authorities. The organization should notify the DFR as soon as possible, but no later than ten (10) business days after a cybersecurity event has occurred. This notification should include the following:

- Date of the event;
- Description of how the information was exposed, including any third-party service providers;
- How the event was discovered;
- Source of the breach, if known;

- Whether or not the organization has notified law enforcement or other regulatory agencies;
- Description of the specific type of information that was compromised (medical, financial, PII);
- The time and scope of the breach, including the total number of possibly affected consumers; and
- Whether any of the information has been recovered.

Notification should also be made to insureds or other parties who have been affected by the breach as soon as possible. This will allow users to mitigate damages (change passwords, freeze credit, etc.) as much as possible. Organizations should have a plan in place detailing how they will release information to the public. Organizations should also ensure that any disclosure will not impede any law enforcement or regulatory investigations. A copy of such notification should be sent to the DFR.