INSURANCE DATA SECURITY CERTIFICATION

NORTH DAKOTA INSURANCE DEPARTMENT
SFN 62101 (Rev. 11-2021)

Name of Entity	CoCode	State of Domicile	
Mailing Address	City	State	ZIP Code

The undersigned, on behalf of the above-named entity, is authorized to complete this certification as to the licensee's compliance with N.D.C.C. § 26.1-02.2-03:

1. The above-named entity has done a comprehensive review of the sensitive information that is in its possession. Based on the sensitive information in its possession, the above-named entity has developed, implemented, and maintains a comprehensive information security program which:
    a. Protects the security and confidentiality of non-public information;
    b. Protects against threats or hazards to the security or integrity of non-public information;
    c. Protects against unauthorized access to or the use of non-public information; and
    d. Periodically re-evaluates the retention of the non-public information and has a method of destruction if no longer needed.

2. The above-named entity has designated the following employee(s), affiliate or vendor who is responsible for the information security program:_____

3. The above-named entity has identified foreseeable threats that could result in a cybersecurity event.

4. The above-named entity has assessed the likelihood of potential damage of any threats, taking into consideration the sensitivity of the non-public information.

5. The above-named entity has assessed the sufficiency of policies, procedures, information systems, and other safeguards in place to manage any threats.

6. The above-named entity has implemented information safeguards to manage threats identified in the above-named entity's ongoing assessment and assess the effectiveness of the above-named entity's key controls, systems, and procedures on an annual basis.

7. The above-named entity has designed its information security program based on its risk assessment and has determined the appropriate security measures in accordance with N.D.C.C. § 26.1-02.2-03(4).

8. The above-named entity's board of directors has acted in accordance with N.D.C.C. § 26.1-02.2-03(5).

9. The above-named entity has established a written incident response plan to respond to and recover from any cybersecurity event. The plan includes the following required items:
    a. The plan to recover the information systems and restore continuous functionality of any aspect of the above-named entity's business or operations;
    b. The internal process for responding to a cybersecurity event;
    c. The goals of the incident response plan;
    d. The definition of clear roles, responsibilities, and levels of decision-making authority;
    e. The external and internal communications and information sharing;
    f. The identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
    g. The documentation and reporting regarding cybersecurity events and related incident response activities; and
    h. The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

I do hereby swear and affirm that the aforementioned statements and information are true and correct.

Officer's Signature	
Title	Date