NEBCA Written Information Security Plan, *Adopted on 1/5/23*

Since the Commonwealth of Massachusetts requires compliance with law, 201 CMR 17.00 201 *M.G.L. c. 93H Standards for the Protection of Personal Information of Residents of the Commonwealth, NEBCA adopted a Written Information Security Plan (WISP) on 1/5/23.*

NEBCA Written Information Security Plan (WISP)

OBJECTIVE: To create effective administrative, technical and physical safeguards in order to protect NEBCA members' non-public personal information and comply with Commonwealth of Massachusetts requirements (201 CMR 17.00 201 M.G.L. c.93H).

The Northeast Border Collie Association ("NEBCA") President shall maintain and supervise the implementation and performance of this comprehensive information security program. This WISP sets forth NEBCA's procedure for evaluating electronic and physical methods of collecting, storing, accessing, using, transmitting and protecting NEBCA members personal information.

201 CMR 17.02 defines "personal information" as a Massachusetts' resident's first name or first initial and last name in combination with one or more of the following information:

a. Social security number;
b. Driver's license or state-issued identification card number; or
c. Financial account number or credit card or debit card number, with or without any required security code access code, personal identification number or password that would permit access to a resident's financial account.

Aside from transporting to our member premises incoming mail containing personal information sent by individuals to our Secretary, NEBCA does not authorize keeping, accessing, or transporting records containing personal information except personal checks with the following exception:

- Personal checks may be transported from the NEBCA Secretary, Calendar Committee or collected when NEBCA merchandise is sold and these checks are sent to the NEBCA Treasurer. The NEBCA Treasurer does not keep photocopies of checks or any other personal information.

NEBCA notes that personal information could be provided to us (via electronic or physical methods of communication) and it is NEBCA's policy to not keep or maintain information for storage and delete or destroy any copies of the information provided.

NEBCA limits the amount of personal information collected to the minimum necessary to accomplish our mission. NEBCA does not obtain the personal information (as defined above) when individuals make donations.

NEBCA Members who violate this WISP will be warned and then instructed on how to comply with WISP. The NEBCA Board of Directors will oversee the taking of protective actions and/or take disciplinary measures if violations continue.

We will review the scope of these security measures annually or when there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

We will document any responsive actions taken in connection with any incident involving a breach of security. Furthermore, NEBCA will review any such incidents and actions taken, if any, in order to consider making changes in business practices relating to protection of personal information. Though the scope of this WISP is specific to Massachusetts residents, it is NEBCA's intention to apply the protections to all NEBCA members regardless of their state of residence.

Breach of Data Security Protocol: NEBCA does not currently maintain personal information as defined in 201 CMR 17.02. In the future, should NEBCA retain personal information and should NEBCA learn of a personal information security breach, the following protocol is to be followed:

1. The Board Chair will be notified in the event of a known or suspected security breach or unauthorized use of personal information.
2. The President shall be responsible for drafting a security breach notification to be provided to the Massachusetts Office of Consumer Affairs and Business Regulation and the Massachusetts Attorney General's office. The security breach notification shall include the following:
    - A description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;
    - The number of Massachusetts residents affected at the time the notification is submitted;
    - The steps already taken relative to the incident;
    - Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
    - Information regarding whether law enforcement officials are engaged in investigating the incident.
3. The President shall be responsible for informing the people whose personal information was breached and referring them to resources on how to protect their personal information. This information would include (but not limited to) and consider the following;

    Consumer's right to obtain a police report
        - Information on how to request a security freeze at no charge
        - Information needed to request a security freeze
        - Information on complimentary credit monitoring services
        - Name of the parent organization and subsidiary organizations affected