Data Security and Protection Policy
BC Brokerage, LLC

1. **Purpose of Data Security and Protection Policy**

    a. The company must restrict access to confidential data to protect it from being lost or compromised in order to avoid adversely impacting our customers and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.
    b. It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.

2. **Scope**

    a. In-scope: this data security policy applies all customer data, personal data, and other company data. Therefore, it applies to every device that is regularly used for email, web access, or other work-related tasks.
    b. Out-of-scope: information that is classified as Public is not subject to this policy.

3. **Policy**

    a. Principles
        i. The company shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively, efficiently, and safely as possible.
    b. General
        i. Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.
        ii. The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.
        iii. Each user shall read this data security policy
        iv. Records of user access may be used to provide evidence for security incident investigations.
        v. Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.
    c. Access Control Authorization
        i. Access to company IT resources and services will be given through a unique user account and complex password. Accounts are provided by the admin.

Passwords are managed by the admin, in a secure password portal box within the CRM.

Requirements for all passwords are expected to be more than 8 characters, one character being capitalized, one character being a numeric number, and one special character (#,$,%,&)

Role-based access control (RBAC) will be used to secure access to all file-based resources

d. User Responsibilities
    i. All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.
    ii. All users must keep their workplace clear of any sensitive or confidential information when they leave.
    iii. All users must keep their passwords confidential and not share them.
e. Application and Information Access
    i. All company staff and contractors shall be granted access to the data and applications required for their job roles.
    ii. All company staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management.
    iii. Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

4. Access to Confidential or Restricted information

a. Access to data classified as ‘Confidential’ or ‘Restricted’ shall be limited to authorized persons whose job responsibilities require it, as determined by the Data Security Policy or higher management
b. Implementing access restrictions lies with the organization's administration.

5. **Technical Guidelines**

The technical guidelines specify all requirements for technical controls used to grant access to data.

Access control methods to be used shall include: f

- Permissions to files and folders
- Role-based access model
- Web authentication rights
- Database access rights$f$
- Encryption

Access control applies to all workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.

6. **Reporting Requirements**

    a. This section describes the requirements for reporting incidents that happen.

        i. Incident reports shall be produced and handled by the admin team

        ii. High-priority incidents shall be immediately escalated

7. **Ownership and Responsibilities**

    a. **Data owners** are employees who have primary responsibility for maintaining information that they own, such as an executive, department manager, or team leader.
    b. **Users** include everyone who has access to information resources, such as employees, trustees, contractors, consultants, temporary employees, and volunteers.
    c. **The Incident Response Team** - Admin of BC Brokerage.

8. **Enforcement**

    BC Brokerage will continuously monitor all systems to assure security.

    Any user found in violation of this policy is subject to disciplinary action.

9. **Definitions**

i. **Database** — An organized collection of data, generally stored and accessed electronically from a computer system.
ii. **Encryption** — The process of encoding a message or other information so that only authorized parties can access it
iii. **Role-based access control (RBAC) -** A policy-neutral access control mechanism defined around roles and privileges.
iv. **Virtual private network (VPN)** — A secure private network connection across a public network.
v. **Two-Step Authentication -** via employee's phone or email address.

10. **Related Policies**

i. Privacy Policy:

BC Brokerage and its affiliates will not sell, trade, or give away your personal information to anyone, except those specifically involved in the referral or processing of your life insurance quote or application. Additionally, we maintain a secure office to ensure that your information is not placed at unreasonable risk. Our guidelines for protecting the information you provide our company, BC Brokerage, appear below. Collection and Use of Information Personal Identifiable Information. To provide you with a life insurance, disability income, long-term care, or annuity quote or to process your application with the insurance company you select, we collect your contact information (email address, phone number, and mailing address), personal health information (you and/or your family's medical history), financial information (occupation, income, and net worth), and demographic information (zip code, gender, and state). Contact, personal health, demographic information, and/or employee information is required by the insurance company to process an application form. This varies by carrier.

Your contact and demographic information may also be used by BC Brokerage and/or its affiliates to get in touch with you when necessary to process your application. Emails and/or phone calls will be used to contact you throughout the application process to inform you of the status and to obtain additional information that is requested as part of the application. Emails, postal mailings, or telephone calls are made upon your request or as a friendly reminder if we have not received the requested information for a prolonged period. If you prefer a different method of communication, a certain time to get in touch with you, or a representative/advisor/trustee who represents you and your

interests, please contact BC Brokerage, IN WRITING, with exact contact information.

Sharing of Personally Identifiable Information

It is our firm commitment to you that BC Brokerage and/or its affiliates will not sell, trade, or give away your personally identifiable or personal health information to anyone, except those specifically involved in the processing of your insurance quote and/or application. Additionally, BC Brokerage and/or its affiliates will (as described below) share your personally identifiable information and/or personal health information only with the following categories of third parties:

- Your chosen insurance company. As stated above, your personally identifiable information is sent by BC Brokerage directly to the insurance company to process your application form.

- Service providers. BC Brokerage may provide your personally identifiable information to reputable service providers who provide routine services such as paramedical exam companies or companies that handle requests for medical records or inspection reports.

- Legal obligations. BC Brokerage may release personally identifiable information, including your personal health information, when we believe, in good faith, that such release is reasonably necessary to comply with the law or a valid court order.

Security

All personally identifiable information collected to provide you with insurance services is securely stored. BC Brokerage employs extensive information protection controls to maintain physical, electronic, and procedural safeguards to protect your personal information. Additionally, access to the information is restricted to select BC Brokerage associates.

Correct/Update Your Information

If you want to correct or update your contact information, simply email or call us, or visit us online at www.bc-brokerage.com.

Please note that once your application has been submitted to your chosen insurance company, you may have to contact the insurance company directly to correct or update your information.

Notification of Changes to the Privacy Policy

BC Brokerage may edit this policy from time to time. You may request a copy of our current policy at any time by email, phone, or postal mail, or find it at www.bc-brokerage.com.

BC Brokerage, LLC
www.bc-brokerage.com | 765.730.7146
PO BOX 441032
INDIANAPOLIS, IN, 46244