PRIVACY & SECURITY POLICY

Our **Privacy & Security Policy** refers to our commitment to treat information of employees, clients, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently, and with respect towards individual rights.

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc. Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

Actions

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)
- Consistent monitoring to ensure policy enforcement
- Annual review of policy and procedures by executive leadership and board of trustees

Breach Notification Process:

- Contact company representative, i.e. CorePLUS, Accessible Solutions, Bloomerang, Texas Health and Human Services, regulatory authorities, and others as identified
- Activate Internal Breach Response Team
    - Determine manner/method in which to notify individuals of suspected breach
    - Work with appropriate authorities and company representatives to resolve the situation

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

Internal Breach Response Team

Incident Lead – Debbie Sheffield
Executive Director – Christine Hockin-Boyd
Information Technology – CorePLUS