1. Purpose

1.1. The purpose of this policy is to establish guidelines and principles for the handling and use of private data belonging to BrainXell and its customers to ensure it remains private and protected.

2. Scope

2.1. This policy applies to all BrainXell employees.

2.2. This policy covers employee training and acknowledgement, requirements for handling private data and ramifications for failure to comply with the principles outlined in this policy.

3. Responsibilities

3.1. Employer and Management

3.1.1. BrainXell and its management must ensure that all employees are trained on this policy and enforce the principles contained herein.

3.1.2. Management must review this policy on a regular basis and update as needed.

3.2. Employees

3.2.1. Employees are responsible for reading, understanding, and following this policy and must document this training in the Employee Training Log.

3.2.2. Employees must review this policy annually and after revisions are made and document in the Employee Training Log.

4. Related Documents

4.1. Forms

4.1.1. FRM-GN-001, Employee Training Form

4.2. Policies

4.2.1. POL-009, Information Technology and Information Systems Policy

5. Definitions and Abbreviations

5.1. Private Data: Information concerning a company or person that can reasonably be expected to be secured from unauthorized access or public disclosure.

6. Introduction

6.1. Data privacy and protection is critical to maintaining the continuous and successful operations of BrainXell and its customers. It is essential that all BrainXell employees are aware of how to access, use, store, disseminate, and dispose of private data, this includes internal BrainXell data, and data that BrainXell collects from customers.

7. Policy

7.1. Training and Acknowledgement

7.1.1. All employees must be trained on this policy as soon as possible after the start of employment.

7.1.2. Training includes reading and understanding this policy, along with any additional material deemed necessary by management.

7.1.3. Employees are to acknowledge they understand and agree to follow this policy by recording this training in the Employee Training Log, which must be signed by their supervisor or other management.

7.2. Requirements for Access, Use, Storage, and Disposal of Private Data

7.2.1. Senior management must authorize all access to sensitive private data originating from BrainXell or its customers.

7.2.2. All devices used to access, view, manipulate, and store private data must be secure. Refer to POL-009, the Information Technology and Information Systems Policy for more information.

7.2.3. Private data is not allowed to be accessed or stored on personal electronic devices.

7.2.4. BrainXell private data is not permitted to be shared without written or verbal consent from senior management.

7.2.5. Customer private data may not be accessed or shared without consent from the customer and senior management.

7.2.6. Customer private data may not be used by BrainXell for any purpose other than for the scope of work agreed to by BrainXell and the customer.

7.2.7. BrainXell may not use customer data for internal use without written consent from the customer.

7.2.8. BrainXell shall keep customer data accurate and up to date.
7.2.9. BrainXell must securely dispose or destroy all customer data when requested to do so and communicate this action to the customer upon completion.
7.2.10. Employees must report, in writing, any breach of private data or suspicion of a breach to senior management.
7.2.11. BrainXell must communicate to customers any breach of data privacy.
7.2.12. BrainXell must investigate the cause of any privacy breach and develop an action plan to prevent a similar breach in the future.
7.2.13. Management is responsible for collecting and revoking access to private data upon the end of individuals' employment at BrainXell.

7.3. Breach of Policy Ramifications
7.3.1. Intentional or unintentional violation of this policy will result in disciplinary action, up to and including termination of employment and legal action as applicable.
7.3.2. The severity of disciplinary action is at the discretion of management, and factors such as intent, scope, severity, and consequence may be considered.
7.3.3. This policy is binding to all current and former BrainXell employees. It is expected and demanded that employees protect private data, even while no longer employed at BrainXell.

8. Revision History

Revision Number	Revision Description
1.0	New Document

9. Approvals

Author Name_Date	Reviewer Name_Date
Michael Colwell_19Jan2023	**Molly Miles_20Feb2023**