## 

DATA BACKUP POLICY

This Data Backup Policy aims to establish guidelines and procedures for the regular and secure backup of all [Organization Name] (the Company) intellectual property data. The policy is designed to ensure that the Company is prepared for any eventuality that could lead to data loss, and to provide a clear framework for the secure storage and access of backup data.

SCOPE

This policy applies to all [Organization Name] employees, contractors, consultants, and third-party vendors who have access to the organization's intellectual property data.

POLICY

All company intellectual property data should be backed up regularly, and backups will be stored securely offsite to protect against data loss in the event of a disaster. Backups will be tested periodically to ensure that data can be restored accurately and completely. Access to backup data will be restricted to authorized personnel only.

**Backup Procedure**

The Company will back up data [insert frequency, e.g. daily or weekly] using automated backup tools wherever possible to ensure consistency and reliability in the backup process. In creating backups, the Information Security Officer (ISO) will:

* Ensure that the backup process captures all company intellectual property data, including files, documents, databases, and applications.
* Verify that the backup data is complete and accurate by conducting periodic test restores.
* Label the backup medium appropriately with the date and time of the backup.
* Store the backup medium in a secure location that is protected from fire, theft, and flood.
* Any data stored on removable media is stored securely when not in use.
* Protect backup data using strong access controls and encryption to prevent unauthorized access.
* Ensure only authorized personnel have access to backup data.
* Train authorized personnel on the backup procedure and emphasize the importance of compliance with the policy.
* Review the backup procedure periodically to ensure that it remains current and effective.

**Data Retention**

To ensure data protection, [Organization Name] will retain data only for as long as necessary. The following data retention periods will be observed:

* **Employee data:** X years after the termination of employment
* **Financial data:** X years after the end of the fiscal year to which the data pertains
* **Customer data:** X years after the last interaction with the customer

After the retention period has elapsed, the data will be disposed of securely. Hard drives and other storage media will be wiped using secure data destruction software, or physically destroyed if necessary. Electronic media will be recycled in an environmentally responsible and secure manner.

**Review and Update**

This policy will be reviewed periodically to ensure that it remains current and effective. Any changes to the policy will be communicated to all relevant parties, and training provided as necessary.