Pacific Associates Cloud Storage Data Security Policy and Procedures

1. Pacific Associates maintains the following requirements for cloud storage:
	1. Data will be Encrypted while on Pacific Associate’s network.
	2. Data will remain Encrypted during transmission to the Cloud.
	3. Data will remain Encrypted at all times while residing within the Cloud storage solution.
	4. Pacific Associates will possess a decryption key for the Data, and the decryption key will be possessed only by Pacific Associates.
	5. The data will only be decrypted until downloaded onto a computer within the control of a Pacific Associates user.
2. Pacific Associates provides annual trainings for all employees working with cloud storage information on how to securely use such information.
3. All employees working cloud storage will be either a user or administrator and abide by the following:
	1. Only administrators can access user information.
	2. All user activity will be tracked by the administrator.
	3. Users will lose access to their cloud storage access:
		1. Upon suspected compromise of the user credentials.
		2. When their employment, or the contract under which the Data is made available to them, is terminated.
		3. When they no longer need access to the Data to fulfill the requirements of the contract.
	4. The administrators will review and verify that only authorized users have access to systems containing Confidential Information.
	5. Medical information can not be stored on cloud databases unless approved by Pacific Associates administrators.
	6. User login and password requirements will include:
		1. A minimum length of 8 characters, and containing at least three of the following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.
		2. Passwords that do not contain a user's name, logon ID, or any form of their full name.
		3. That a password does not consist of a single dictionary word. A password may be formed as a passphrase which consists of multiple dictionary words.
		4. That passwords that are significantly different from the previous four passwords. Passwords that increment by simply adding a number are not considered significantly different.
		5. When accessing cloud information remotely users will only use laptops or tablets approved by Pacific Associates.
4. When contracted work has been completed or when the data is no longer needed. Cloud data shall be returned to the funder or destroyed.