GUAM BEHAVIORAL HEALTH AND WELLNESS CENTER
REVIEW AND ENDORSEMENT CERTIFICATION

The signatories on this document acknowledge that they have reviewed and approved the following:

[x] Policies and Procedure	**Submitted by:** Information Technology Department
[ ] Protocol/Form	**Policy No:** AD-MIS-02
[ ] Bylaws	**Title:** Password Management Policy

Reviewed/Endorsed	**Date**	**Signature**
	6/2/2017	
Title	**Name Title**	Fred Borja Computer System Analyst I
Reviewed/Endorsed	**Date**	**Signature**
	6/2/17	
Title	**Name Title**	Benny A. Pinaula GBHWC Deputy Director
Reviewed/Endorsed	**Date**	**Signature**
	JUN 0 2 2017	
Title	**Name Title**	Rey M Vega GBHWC Director

GUAM BEHAVIORAL HEALTH AND WELLNESS CENTER		
TITLE: Administrative Safeguards: Password Management	**POLICY NO:** AD-MIS- 02	Page 1 of 2
RESPONSIBILITY: Information Technology Administrator (HIPAA Security Officer)		
APPROVED BY:__________ DIRECTOR	**EFFECTIVE:** JUN 0 2 2017 **LAST REVIEWED/REVISED:**	

PURPOSE:

To implement procedures for creating, changing and safeguarding passwords.

POLICY

A. Guam Behavioral Health and Wellness Center in compliance with the password management implementation specification, defined within the Security Awareness and Training Standard in the Administrative Safeguards category of the HIPAA Security Rule § 164.308(a)(5) shall;
   1. Implement periodic security updates, and require that all passwords must be changed at least once every 180 days.
   2. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
   3. All staff shall follow the guidelines in the creation, changing and safeguarding the password.

B. Staff must not share their password with anyone, including administrative assistants or secretaries, unless otherwise justified and approved by the Director or the IT Administrator. All passwords are to be treated as sensitive, confidential information.

C. Training shall be provided to all users and abide by the established guidelines for creating and changing passwords during periodic change cycles.

D. The IT Administrator shall ensure the implementation of the Password Management Policy.

PROCEDURE:

Obtaining system access: User ID and Password for new employee

1. Department Head submits request to the Information Technology (IT) Department identifying and authorizing employee(s) to access what system and what application, and defining the job function and access limitations.
2. Once activated, employee(s) will receive instructions from IT Department on how to change their passwords. Employee(s) should comply with this policy in the frequency of changing their Passwords.

Disabling and terminating authorized user system access

1. IT administrator shall disable and suspend the employee(s) user account if not in use for more than 30 days, until they notify IT Department.
2. When employee(s) terminate their employment and clear-out from the Department of Guam Behavioral Health and Wellness Center, IT Department will immediately remove the employee(s) user access account and password on their last day of work.