Section: Information Technology	Policy Name: **Permissions Management**	Policy Number: **17.02**
Owner: **Chief Information Officer**	Reviewed By: **Natalie Spivak**	Total Pages: **4**
Required By: ☐ **BBA** ☐ **MDHHS** ☐ **NCQA** ☐ **Other (please specify):** _____	Final Approval By: *Natalie Spivak*	Date Approved: Dec 9, 2020
Application: ☒ **SWMBH Staff/Ops** ☒ **Participant CMHSPs** ☒ **SUD Providers** ☒ **MH/IDD Providers** ☒ **Other (please specify):** **SWMBH Guests**	Line of Business: ☐ **Medicaid** ☐ **Healthy Michigan** ☐ **SUD Block Grant** ☐ **SUD Medicaid** ☐ **MI Health Link** ☒ **Other (please specify):** **Internal**	Effective Date: **12/4/20**

Policy: Network permissions are an essential component of security administration. Permissions outline the type of access (read/write) to specific data and documents stored on the network. Careful deliberation and control are essential to successful permissions management.

Purpose: To define and document Southwest Michigan Behavioral Health (SWMBH) network permissions management.

Scope: All SWMBH staff, Community Mental Health (CMH) agencies, Integrated Care Organizations (ICO) and others accessing SWMBH systems.

Responsibilities: Chief Information Officer (CIO) or his/her designated Administrator – Add, delete and modify network security permissions**.** Business Analyst – Responsible for administering electronic medical record (EMR) security

Definitions:

A. Administrator is the CIO or his/her delegated administrator.

B. Active Directory (AD) is a Microsoft technology used to manage access controls of computers and other devices on a network.

C. Security group – Collection of user accounts and/or devices which are granted the same security permissions. Security groups provide an efficient, simple and more secure method to assign resources on a network.

D. SWMBH Help Desk – SharePoint site which serves as intake mechanism for all Information Technology requests.

E. Network Permissions are login access to any network resource that includes the file server, databases, SWMBH Portal, Tableau, or any web-based applications such as LOCUS, SIS Online, CC360, CMT, etc. to which SWMBH information technology (IT) manages user access.

F. Duo Mobile - secure method of two-factor authentication. Users verify their identity by approving push notifications on their mobile phones before being granted access to critical applications.

Standards and Guidelines:

All network permissions will be approved by the CIO (or his/her designated Administrator). In accordance with CIO approval, responsibilities will be as follows:

A. Administrators will make every effort to administer security permissions using security groups. Individual permission assignments will be at the discretion of the CIO (or his/her designee).
B. Administrators will be responsible for basic AD administration including security group administration, staff onboarding, offboarding, granting permissions, adding and deleting members from SWMBH distribution lists, granting/revoking folder permissions, managing SQL Server access to data, managing inheritance, moving folders, audits, etc.
C. Network access will automatically be disabled if more than 45 days of inactivity. Login accounts that have been disabled can only be enabled again by making a request to the CIO or his/her designated administrator.
D. Users requiring access to critical applications such as Microsoft Dynamics financial systems and Windows or SQL servers are required to use two-factor authentication: a user ID and password and Duo Mobile or equivalent SWMBH CIO approved product for authentication.

Procedures:

A. All internal (SWMBH staff) AD permission change requests (distribution list changes, SharePoint Access, Tableau access, etc.) require Senior Leader (SL) approval and submitted through Supervisor Requests located on the SWMBH Portal Help Desk. It is expected that the requesting SL will solicit pre-approval from other SL's who are responsible for the security/data/committee being requested.
B. All external (non-SWMBH staff) security requests will be submitted to the CIO (or his/her designee) via email. External requests are required to originate from an appropriate business email domain (i.e. gmail.com, yahoo.com, att.net, etc. are not acceptable) to be eligible for processing. Requests must include the following: full name, description of permission requirements, name of SWMBH Senior Leader sponsor.
C. Permissions change requests submitted through the SWMBH Help Desk are expected to be completed within 8 business hours. Exceptions may occur due to complexity, resource availability, or organization imperative.

References: SWMBH Policy 17.05 Network Password Requirements

Attachments: None

Revision History

Revision #	Revision Date	Revision Location	Revision Summary	Revisor
	3/29/2019		Initial Release	R Paruch
1	3/10/2020	Reviewed by	Changed Rob Moerland to Natalie Spivak	N Spivak
1	3/10/2020	Date Approved	Added	N Spivak
1	3/10/2020	Definition D Definitions F	Changed Information Technology Solutions ITS to Information Technology Added Definition of Duo Mobile	N Spivak
1	3/10/2020	Standards & Guidelines	Added Paragraph D Changed designate to designee	N Spivak
1	12/4/20		Reviewed for NCQA	N.Spivak

17.02 Permissions Management

Final Audit Report 2020-12-09

Created:	2020-12-09
By:	Erin Peruchietti (erin.peruchietti@swmbh.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAXDbK0d8Q5dNKOBWr8CVUlCtuVwieX_dc

"17.02 Permissions Management" History

Document created by Erin Peruchietti (erin.peruchietti@swmbh.org)
2020-12-09 - 3:12:44 PM GMT- IP address: 96.36.47.106

Document emailed to Natalie Spivak (natalie.spivak@swmbh.org) for signature
2020-12-09 - 3:13:03 PM GMT

Email viewed by Natalie Spivak (natalie.spivak@swmbh.org)
2020-12-09 - 4:16:37 PM GMT- IP address: 104.47.36.254

Document e-signed by Natalie Spivak (natalie.spivak@swmbh.org)
Signature Date: 2020-12-09 - 4:17:04 PM GMT - Time Source: server- IP address: 24.247.148.221

Agreement completed.
2020-12-09 - 4:17:04 PM GMT