PROCEDURE TITLE	File Access Control Approval Procedure	**DOCUMENT ID**	ADMIN-RM-0251.02
OWNER	Vice President of Business Administration	**CREATION**	05.31.2024
STANDARDS AND REGULATIONS	**COA:** RPM 4, RPM 5, RPM 5.01, RPM 5.02 **Admin Code:** **Statute:**	**RENEWAL DATE**	09.2028
RELATED OMC POLICIES / PROCEDURES	Network Access and Authentication Policy	**LAST MODIFIED/ APPROVAL**	07.2026 - Chief Financial Officer
APPLICABLE TO	1 – All Staff 8 - Volunteers	**EXPERT REVIEW**	

PURPOSE

This procedure is to specify guidelines for the approval process to grant access to data on the One More Child network.

FORMS AND REFERENCE DOCUMENTS

Title	Description

PROCEDURE

File access control is a data security technique that limits system access based on the user's specified authorization. There are many distinct types of data stored in the One More Child (OMC) network. Some of this data is of a sensitive business nature (Human Resources data, financial data, etc.), some is a part of a protected class of data (Protected Health Information, Personally Identifiable Information, etc.), and some is data that is department specific. OMC uses a combination of methods to manage the security of all data on the OMC network.

Access Control Systems
OMC uses a combination of two major Access Control Systems for the security of data on the OMC network – Mandatory Access Control, and Role-based Access Control. Mandatory Access Control uses individual network accounts to grant permissions to specific locations. Instead of individual user assignments such as in Mandatory Access Control, Role-based Access Control programs user permissions based on their position (role) in the organization. Each role in an organization is provided with a customized level of access rights. Users are then assigned to a role and inherit those access rights. In most cases in the OMC network, these roles are based on the assigned department. In both cases, File Access Control Permissions are assigned by the Information Technology Department.

Separation of Data Types
OMC utilizes Microsoft SharePoint sites for data storage and security. In the OMC network, permissions are set at the Document Library level inside each SharePoint site. The same permissions are applied to each folder and file in that library. This needs to be considered when granting authorization for file access permissions.

Authorization Needed
As much as possible, Role-based Access Control has been used to grant File Access Permissions to the Document Libraries. Where Role-based Access Control is used, the grant of permissions occurs when a person is assigned to a home department by Human Resources. The assignment triggers an automated process that applies pre-assigned permissions based on the department role (position title) selected.
Where Role-based Access Control is not used, authorization for libraries is controlled under the Mandatory Access Control system. The Mandatory Access Control system is used when there is not a specific role that applies to everything in a Document

Library. This method is also used to grant permissions to Role-based Access Controlled libraries when persons are not assigned to the home department or an associated role for them.

Granting Authorization
Due to the complex and varied nature of the data on the OMC network, permissions must be authorized at the Executive Director level or above for the department that "owns" the data.

Examples:

- Authorization for someone in the Southwest Foster Care office needing access to files in the Central Florida Foster Care Document Library would need to be approved by the Executive Director of Foster Care. If that person is unavailable, the appropriate Vice President of Program Operations would need to authorize access.
- Authorization for someone in the Global department needing access to files in a Human Resources Document Library would need to be approved by the Chief Financial Officer.

Obtained approval can be sent to the Information Technology Department via email. Once the appropriate approval is received, the change in File Access Control permissions will be made.

Enforcement
Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties, up to and including termination of employment. Where illegal activities or theft of property (physical or intellectual) are suspected, OMC may report such activities to the applicable authorities.