

Appendix B – File Migration and Technical Guidance

Intent

Garrison IMO provides the following technical guidance and recommendations for Garrison organizations to execute a systematic, organized, and timely migration of all organizational files and data from legacy file-share services hosted by the Fort Sill Local Network Enterprise Center (LNEC) to the Army's enterprise A365 SPO Org-Data services. This guidance is geared to the lowest level organization and individuals to execute the migration. These are the people most familiar with the laws, regulations, and policies for data in their realm, most aware of the operational impact of the data, most involved in processing the data, and most impacted if the data isn't migrated, organized, and accessible post-migration. Reference 'Appendix A – Roles and Responsibilities' for roles, responsibilities and terms used in this document. This migration should be completed in three phases:

- Identify all file-shares, all organizational data, all stakeholders, and all available A365 SPO-Org-Data resources.
- Organize files and data in folder structures that match each destination, make data easy to find post migration, and make each migration one drag-and-drop per destination. Audience and access permissions determine destination. Do not migrate unnecessary files and data or folders and files not following ARIMS guidance and naming conventions.
- Migrate the organized files to the predetermined SPO Org-Data destination. Verify all folders/files are in the appropriate location with the right permissions. Socialize the migration with the intended audience.

These phases are further detailed below.

Phase I: Identify File-shares, Resources, and Stakeholders.

Organizations may have data stored in multiple file-shares, for example, "\\SILLA7NEC462004\dca" file-share and "\\SILLA7NEC462004\dmw" file-share. Identify all file-shares used throughout the organization and process each file-share individually and completely. Reference the list of file-shares at the end of this section.

Organizations should identify all stakeholders responsible for files stored in their file-shares prior to migration to ensure organizational files and data at all levels in that file-share are accounted for and correct permissions are applied. Stakeholders will include:

- Record Manager and Record Coordinators on appointment orders for the purpose of checking ARIMS compliance.
- DPTMS Security Manager and Security Manager POC's for the purpose of checking CUI, PII, PHI.
- Site Owners (SO) and Content Managers (CM); subordinate elements using part of the file structure for their data and files.
- Individuals with additional duties storing government files for their organizations.
- Leaders storing performance evaluations and counselling forms.

Personnel executing the migration must have 'Read' access to all files and data they need to migrate and 'Write' access to the destination locations in SPO Org-Data. Folders with limited access may contain CUI, or other restricted access information that is more appropriate for an individual to store in their OneDrive or requires access considerations in the SPO Org-Data File-Share. The SPO Org-Data files share is authorized for CUI, PII and PHI, but the data should be active and up to date and not obsolete. For CUI, PII and PHI that is no longer needed, check with your Records Coordinator and/or the Garrison's Records Manager and the organizations Security POC or the DPTMS Security Branch as to the best way to store data that is considered inactive or no longer needed.

Identify organizational resources to assist with the migrations:

- IMO, Directorate Site Owners (SO) and/or Content Managers (CM) in an enablement and admin role provides general IT and Teams admin support consisting of initial file-share group permissions and overall SPO support to the entire Garrison.
- ARIMS Site Owners in a Records Manager or Records Coordinator role, identify official records, inform how to apply the ORL to those records, provide guidance on how data is managed, and ensure data is properly stored after the migration.
- Security Manager POCs within the organizations and DPTMS Security Branch should assist organizations as to proper storage of their CUI, PII, PHI data. DPTMS Security Managers may be given permissions to any folder or file within the SPO Site Page (AKA Web Pages) or SPO Org Data site collections for the purpose of policing folders and files for CUI, PII, PHI infractions or non-compliance.

Garrison IMO hosts these file-shares:

- \\SILLA7NEC462004\agd *MWR Proponent
- \\SILLA7NEC462004\asp *DHR Proponent
- \\SILLA7NEC462004\dca *PAIO Proponent
- \\SILLA7NEC462004\asd *MWR Proponent
- \\SILLA7NEC462004\chp *RSO Proponent
- \\SILLA7NEC462004\deq *DPW Proponent
- \\SILLA7NEC462004\des *DES Proponent
- \\SILLA7NEC462004\dmw *MWR Proponent
- \\SILLA7NEC462004\dpw *DPW Proponent
- \\SILLA7NEC462004\gis *DPW Stays on LNEC Share
- \\SILLA7NEC462004\irc *IRACO Proponent
- \\SILLA7NEC462004\pai *PAIO Proponent
- \\SILLA7NEC462004\psb *DHR Proponent
- \\SILLA7NEC462004\saf *SAF Proponent
- \\SILLA7NEC462004\smo *PAIO Proponent
- \\SILLA7NEC462004\dpt *DPTMS Proponent
- \\SILLA7NEC462004\eeo *EEO Proponent
- \\SILLA7NEC462004\gc-grp *GCMD Proponent
- \\SILLA7NEC462004\imo *IMO Proponent
- \\SILLA7NEC462004\mob_bde *PAIO Proponent
- \\SILLA7NEC462004\rmo *RMO Proponent
- \\SILLA7NEC462004\sjja *PAIO Proponent

This Phase will end with once Organization(s) have cleaned up data on shared drives and the Installation Records Manager Shauki Holmes, (580) 442-6573, shauki.m.holmes.civ@army.mil reports to the IMO Shane Babb, (571) 644-3758, martin.s.babb.civ@army.mil or Noel Arroyo-Carreras, (580) 442-3490, noel.arroyocarreras.civ@army.mil.for that respective Organization to progress to Phase II.

Phase II: Organize and Plan your move.

Start by analyzing your current shared drive contents to determine what data needs to be migrated, where to move the files and what can be archived/deleted.

- For files currently used for planning/short term collaboration, store on MS Teams.
- Anything pertaining solely to the individual should be moved to that individual's OneDrive; this includes training records, individual evaluations, etc
- Anything still in draft, containing PII, or internal to the organization should all go to an internal only SharePoint Org-Data library. This library will only be accessible by members you designate within your organization. **NOTE:** IMO and Organizational Site Owners (SO) can assist with the creation of that internal library.
- Records should be handled in accordance with (IAW) the Army Records Information Management System (ARIMS). For more information about ARIMS, <https://www.arims.army.mil/arims/default.aspx> or contact your organization's Record Coordinator (RC) or the Garrison DHR Records Manager (RM).
- Any information used from external collaboration and dissemination should go into a SharePoint Document Library for CAC "public" access. This library can be set to "read only" for customers; meaning visitors to the Document Library on their SharePoint site pages (AKA web pages). Public CAC Document Library visitors can only read and download documents: they cannot alter, edit, or delete content. **NOTE:** Organizational Site Owners (SOs) or Content Managers (CMs) can assist with the creation of that public library. The SPO Site pages link is <https://armyeitaas.sharepoint-mil.us/sites/IMCOM-ID-T-USAG-Sill>.


For further information/guidance visit the **Garrison Read Me | How To Videos** link on the Garrison SPO Org-Data Site: <https://armyeitaas.sharepoint-mil.us/sites/IMCOM-ODT-Sill?web=1>

This Phase ends when Site Owner(s) have folders and permissions established for their entire organization and report to the IMO ready to migrate.

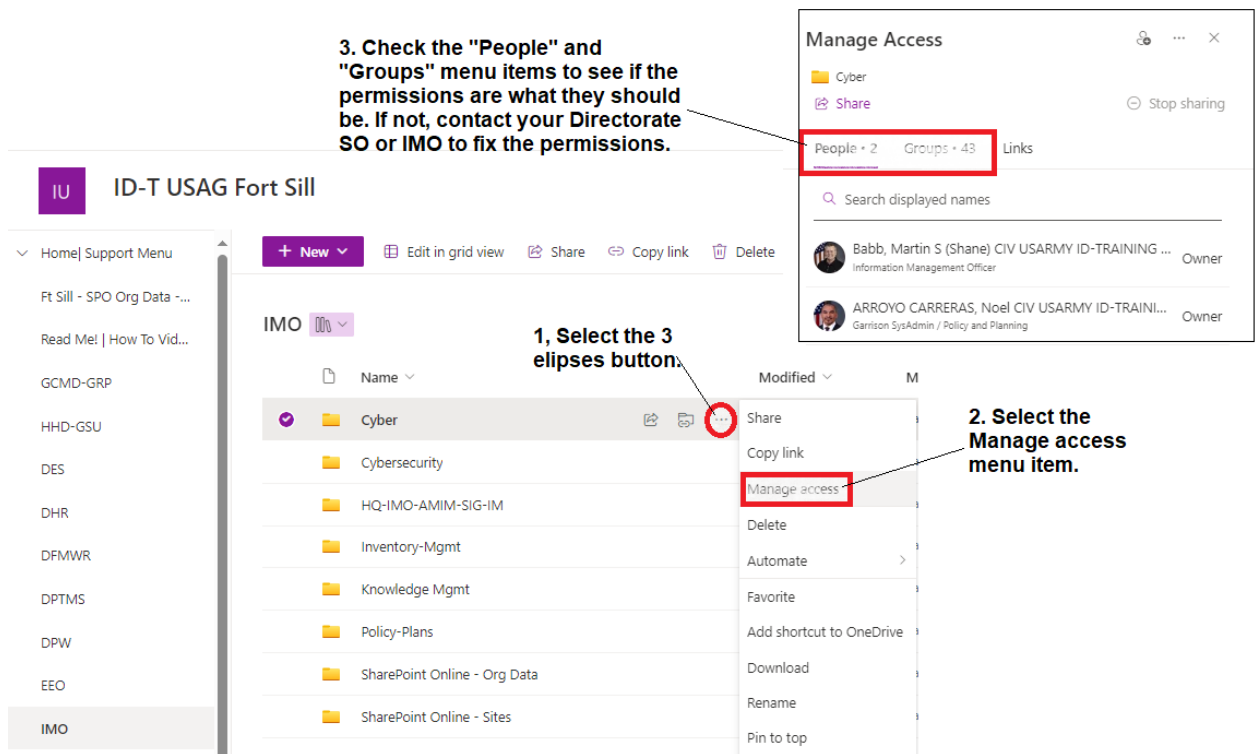
Phase III: Migrate Files and Validate:

This is as simple as a "drag and drop" between the shared drive and the new SharePoint Org-Data Document Library.

- Navigate to your SharePoint Document Library site by visiting the following site: <https://armyeitaas.sharepoint-mil.us/sites/IMCOM-ODT-Sill?web=1>
- Find your Organization left navigation menu and open it. Find the folder or sub-folder you want to copy & paste or drag & drop to and open it.

- In a separate window, open your old LNEC Share-Folder and files using the **Windows File Explorer** that is built into Windows. **Pro Tip: Hold down the “Windows” key on your keyboard and tap the “E” key quickly to open the Windows File Explorer.**  **+E**
- Once you have the File Explorer open, use **CTRL-A** to highlight all folders or **CTRL-click** to highlight specific folders, drag them into the SharePoint Document library, and drop them (drag & drop).
- The folder structure (including all sub-folders) will remain intact. Be patient.
- Validate that you have moved all organizational folder & files to the intended Document Libraries.
 - Check that the permissions set for your specified folder is set up correctly. Here’s how in 3 easy steps:

3. Check the "People" and "Groups" menu items to see if the permissions are what they should be. If not, contact your Directorate SO or IMO to fix the permissions.



1, Select the 3 elipses button.

2. Select the Manage access menu item.

3. Check the "People" and "Groups" menu items to see if the permissions are what they should be. If not, contact your Directorate SO or IMO to fix the permissions.

- If you are unable to do the above task, get with your Directorate SO or IMO for support.

This Phase ends when IMO and Installation Records Manager have inspected the folders and determined folder and files have been migrated properly and have been Validated with IMCOM migration process.