



**USAID**  
FROM THE AMERICAN PEOPLE



# EISA FOLDER STRUCTURE GUIDELINES AND RECOMMENDATIONS

9/1/2006

This publication was produced for review by the United States Agency for International Development. It was prepared by BearingPoint, Inc.

# **EISA FOLDER STRUCTURE GUIDELINES AND RECOMMENDATIONS**

TECHNICAL ASSISTANCE FOR POLICY REFORM II

CONTRACT NUMBER: 263-C-00-05-00063-00

BEARINGPOINT, INC.

USAID/EGYPT POLICY AND PRIVATE SECTOR OFFICE

9/1/2006

AUTHOR: D. JONATHAN TOMAR

## **DISCLAIMER:**

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

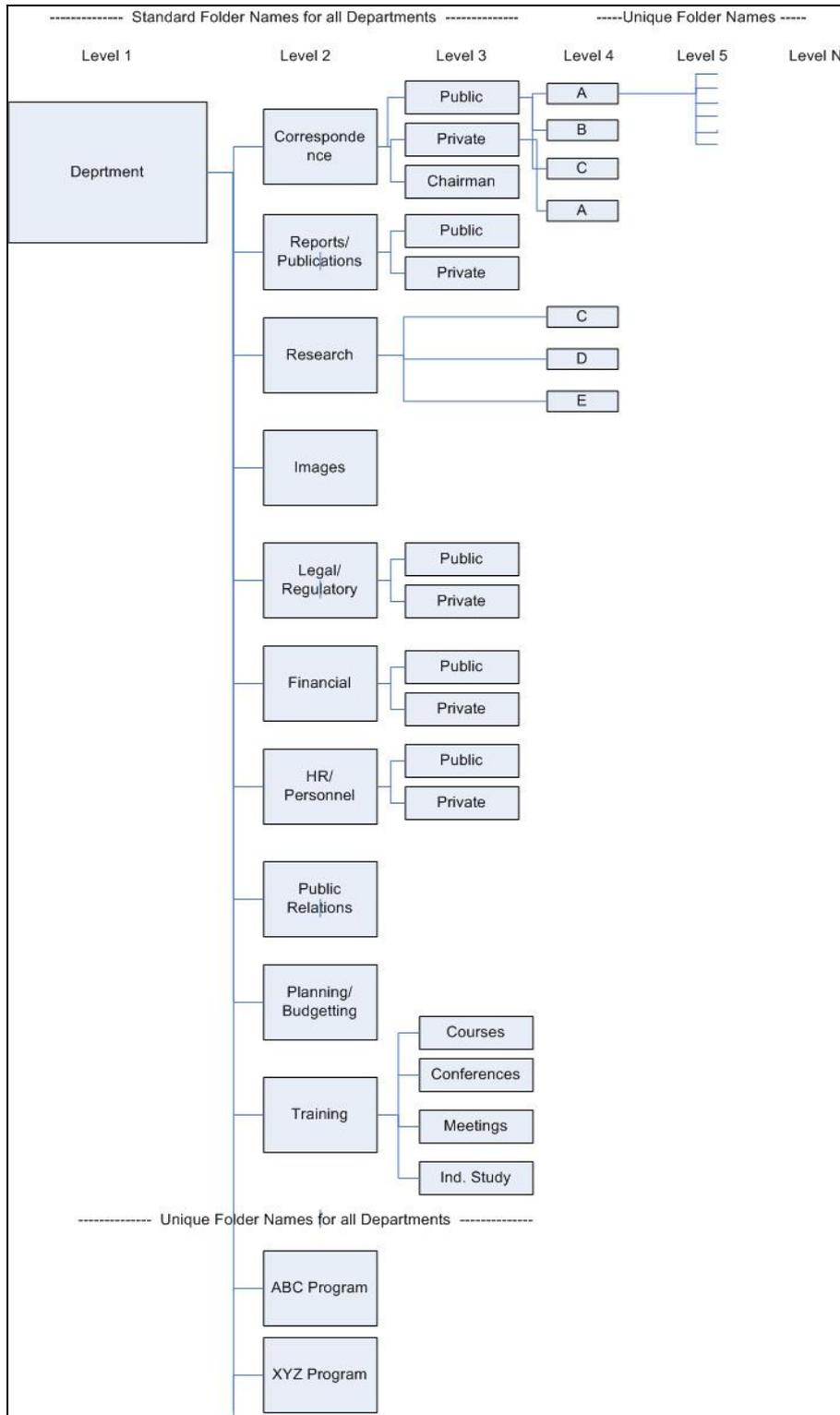
## 1.0 INTRODUCTION

The purpose of this report is to present a workable folder/directory structure model for EISA.. It is important to stress “workable” since any structure that is too complex will soon be discarded by participants. At the same time, we want a structure that is organized coherently so it can assist EISA in the sharing of information between departments.

It is important that the file structure correspond closely with the “group” structure in active directory. This will facilitate the creation of meaningful and understandable access privileges. It is important that information be shared across departments and this structure should facilitate this sharing. At the same time, there is a need for confidentiality among departments and individuals. The organization must have some privacy in order to facilitate honest dialogue and finding that balance will be a difficult task.

The rules and directions set forth are only to be used as a starting point for discussion. It is expected that some of the structure will be changed as different groups consider the structure and give input. In any undertaking of this type, no one will be completely satisfied with the design. It should be permissible to modify the structure to better handle the anomalies and special situations.

## 2.0 CONCEPTUAL DESIGN



The design is based on the following component parts.

**Level 1- Department or Major Item** – The highest level in the structure. This will be immediately below the root level. These major groupings would include each department at EISA (registration, IT, Legal etc.). In addition to the department level there would be certain other major categories which would be on the same level as departments. These would be major affiliated organizations like USAID, World Bank, Ministry of Investment. In addition, there would be other major items such as disasters, special events, task force activities etc. These would be identified by key individuals in the organization and then communicated to the IT department to create the folder and the group.

**Level 2 – common folders** - The second level should contain a set of folders common to all departments and major items. In some cases not all of these folders will be necessary. Some examples of these common level 1 folders would be:

- Correspondence
- Reports and Publications
- Research
- Training

**Level 3 – common folders** – The third level should contain common folders pertinent to the level 2 folder. For example, under correspondence there would be:

- Public
- Private
- Chairman

**Level 4 – unique folders** – there would be no common folders under level 3. Anything after this level can be defined for a department or a major item. For example, under folder IT department\Research\ we could have several sub folders like:

- Networking
- Internet security
- Scanning technology
- VOIP

**Level 5 ... Level n - unique folders** – there should be no limit to the number of sub folders in the structure. The limitation should be practical (the difficulty of managing a long folder structure is cumbersome). An example of an acceptable folder structure could be :

IT department\research\networking\vista\installation

**Unique Department Folders** – In addition to the standard folders, departments would be allowed to create their own unique folders at level 2. These folders would be created for areas of activities unique to that department that do not fall under the common folders. Care should be exercised to make certain that these folders are not duplicates of existing common folders. In addition, if several departments use the same unique folders they should be standardized and added to the common folders.

**Major Items** – There will be activities that do not fall under a specific department and require a high degree of coordination. These items may be placed at the same level (level 1 ) as a department. Examples of a major item may be a task force working on a major problem that involves several staff in several departments.

While it is not recommended to establish new groups for every task force, it may be necessary from time to time to establish new security groups with individual user or group access rights.

It will be important to assess these new folders and determine if they are still relevant and to archive and remove them when they have become obsolete.

### **3.0 DEPARTMENTS AND MAJOR ITEMS**

The following is a list of the major departments at EISA which will be used to establish a level1 folder:

- Chairman
- Deputy Chairman
- Re-insurance Dept.
- Property & Liability Dept.
- Life Dept.
- IT Dept.
- Research Dept.
- Library
- Central Statistics Dept.
- Investments Dept.
- Financial Analysis Dept.
- Pension Funds Dept.
- Managing Affairs Dept.
- Financial Affairs Dept.
- Register Dept.
- Life Actuarial Dept.
- Non-Life Actuarial Dept.
- Governmental Fund
- Follow Up Dept.
- Legal Dept.
- Public Relation Dept.
- Training Dept.

- Policy Holders Dept.

In addition, the following major item folders can be established:

- USAID
- Ministry of Investment
- Ministry of Administrative Developing
- World Bank
- Major disasters (train crash, boat sinking, fires, etc. )

#### **4.0 PRIVILEGES**

There are basically four categories of user privileges defined as groups within the active directory. These are:

- All Users – AU
- All Managers – AM
- Group (Department) Users – GU
- Group (Department) Managers – GM

It would be permissible to define other groups as necessary. Example of this might be members of a task force or committee. This will be necessary for access rights to major item folders. Within groups privileges can be defined as read only, read/write, etc. as necessary. Domain administrators should not have rights to view confidential information. It is important that rights not be defined at the user level.

In general, we should err on the side of being too liberal with rights. It is not recommended to use denial of rights as this can develop very complex relationships. Also, rights should be inherited, such that user of the main folder should have access to all subfolders unless the group has been specifically removed or altered.

No user should store any organizational information or data on the local C: drive. This can be used for temporary files and files that are not germane to the operation of the department. All important information should be stored on the server. Local C: drives should never be shared. Extremely sensitive files should be protected by other means such as password protection within the software or encryption. The operating system should not be considered adequate for extremely sensitive information.

#### **5.0 APPLICATIONS**

This folder structure can be used for the following applications:

- Windows folder structure (Windows Explorer)
- Exchange Public Folders
- Document Management System

The primary application of this structure will be in the establishment of the Windows folders on the server.

In addition, the Exchange public folders should adhere to the same structure.

When the document management system is selected and implemented the same structure should be imposed on it. It remains to be seen if the document management system can work with the Windows active directory, but if not, then the same group structure should be replicated in the document management system.

## **6.0 FILE NAMING CONVENTION**

It is recommended that no strict file naming convention be applied. This does not mean that any names used are acceptable. The following general rules should apply.

- File names should be sufficiently descriptive to explain the content of a file.
- All user profiles must be maintained accurately so the authors name will appear in the author name property.
- The date and time must be accurate on the files. No back dating of files is allowed.
- Important files which will be shared by other users/departments such as reports must also contain the title, subject, keyword and comment properties to accurately describe the document in greater detail.
- Computers should be configured to show the detailed information in the detailed folder view.
- All files should be entered into the document management system.
- File information can be in Arabic or English. The detailed information must be entered in the same language as the file name.
- Keywords should be standardized.
- E-mails should have specific descriptions in the subject line describing the e-mail in some detail. All emails should be moved from the inbox to the the appropriate folder after being read. Insignificant emails should be deleted immediately

## **7.0 RETENSION SCHEDULE**

Equally as important to having an organized folder system is the removal of outdated files and e-mails. It will be difficult to enforce a strict deletion policy. One way to do this with out too much difficulty is to create an archival area where files are automatically moved after a certain period of time. Once in the archival area they then can be moved to offline storage after another period of time. This will require a significant effort on the IT department to maintain this discipline. However, it will save space, reduce delay and difficulty in locating files and speed up processing time.

This is particularly useful for e-mail archiving. As people start using e-mail some people will begin to horde emails. This will start to use up valuable space as thousands of junk emails are left on the server. Enforcing required purging of e-mail is necessary.

It is essential to establish good habits early in a person's use of email and the document management system. It is critical that policies be established and explained to users during initial training on these applications.

## **8.0 RELOCATION OF MY DOCUMENTS**

Another important issue is the relocation of the my documents folder or the default location for files to be saved. The options are:

- C:\my documents
- F:\users\user\_name
- F:\department

It is recommended that the default location for files be the f:\department folder. This will encourage user to store documents on the server (which we prefer) and to store them in an organized and easily shareable folder structure.

Another issue will be the location of the individual mail store in Outlook. Exchange has the ability to store information in a local .PST or in an exchange store on the server. By default the Outlook points to a local .PST. It is important to remap the store to the server. If the mail store is directed to the local drive no backup of email will occur.

## **9.0 DOCUMENT MANAGEMENT SYSTEM**

Implementing a full document management system will be a difficult task for EISA. For a system to be truly effective it will be necessary for most if not all documents to be entered into the DMS. This will require every document be properly labeled with the appropriate meta data information (name, title, author, keywords etc.). Enforcing this discipline will be difficult.

It would be optimal to introduce the new DMS concurrently with the new servers and new network. It would be best to have the structure in place at the outset of the new system so training could include the new DMS at the same time as the other new applications.

It is recommended that the IT department hire at least one person to be responsible exclusively for the new DMS. This position will be responsible for a number of activities related to the DMS including.

- Manage the organization of the cabinets, drawers, files etc. of the new system to insure that all departments have a meaningful folder structure before and after the implementation phase.
- To recommend and implement changes to the overall structure of the DMS as situations change and new items are added.
- To provide detailed technical assistance to all users and to the IT staff on all aspects of installing, maintaining and using the DMS.
- To plan and implement all future enhancements to the system including the integration with the website and introduction of work process rules.
- To develop and enforce a workable file retention program and to perform the routine maintenance to archive and remove old documents from the system
- To provide user training in all aspects of the DMS including the scanning of documents, adding of emails, document searching, integration with active directory and exchange.
- Implementing and maintaining the security parameters of the system including user and group settings and privileges.

## **10.0 MIGRATION OF CURRENT DOCXPLOERER FILES**

It is recommended that the current DocuXplorer files not be imported or migrated to any new document management system. The reasons for this are:

- There is currently very little access of archived files – There appears to be very little if any access of existing archived files
- There would be no automated way to export the metadata – There is no “easy” way to export the metadata from the current system without significant programming effort. Currently, we do not know the technology which will be used by the new DMS so it will be impossible to design and test the system at this time. If a method for migration is developed it should still be considered carefully whether to perform the migration.
- There is an export function in the DocuXplorer but it would be exceedingly slow and cumbersome. – Individual files can be exported to the tiff format but without any metadata. In addition, once the file is exported it would have to be imported into the new DMS and all the metadata would need to be entered at that time.

It is recommended that the IT department test the availability of running the current system on the new server under Windows XP and see if it can run. In this way the old documents could be accessed via the old software. When the new DMS is installed, then new

documents would be entered into the new system only. Therefore there would be a transition date after which all documents would be entered into the new system only.

## APPENDIX – DETAILED FILE STRUCTURE

Note: Common structure to be used for:

1. Windows Explorer
2. Exchange Public Folders
3. Doc. Flow System

AM - All Management  
 GM - Group Management  
 GU - Group users  
 AU - All users

Major Items: (they do not have the same structure as departments)

USAID

Ministry of Investment

Ministry of Administrative Developing

World Bank

Major disasters (train crash, boat sinking, fires, etc. )

<u>Departments</u>	Level 1 Common Folders	Level2 Common Folders	Level3...Level n Unique Folders	Access Rights	Type of documents
Registration					
	Correspondence	Public	by category, matter, company	AU	Internal memos, letters, e-mails, and brief text documents sent within EISA (generally under 3 pages)
		Private	by category, matter, company	AU	Memos, letters, e- mails, and brief text documents sent within EISA (generally under 3 pages)
		Chairman	by category, matter, company	GM	Memo's, letters, e-mail correspondence with the chairman of EISA
	Report/Publications	Public	by category, matter, company	AU	Word documents, PDF files etc. that are generally longer then 3 pages and are meant for EISA staff
		Private	by category, matter, company	AU	Word documents, PDF files etc. that are generally longer then 3 pages and are meant for the general public

Research		by category, subject matter	AU	<p>General data downloaded from the web for various purposes as reference material</p> <p>Any graphic images used by the department for reports, websites etc.</p> <p>Documents pertaining to laws, decrees and regulations that can be made available to the general public</p> <p>Documents pertaining to laws, decrees and regulations that can not be made available to the general public. E.g. policy recommendations, opinions etc.</p> <p>Documents related to financial issues within EISA or the department that can be shared with all users in EISA</p> <p>Documents related to financial issues within EISA or the department that can not be shared with all users in EISA</p> <p>Human resource information available to all users in EISA such as information about new hires, work rules etc.</p> <p>Human resource information not available to all users in EISA such as performance reviews, hiring information etc.</p>
Images		e.g. by category or purpose	AU	
Legal/Regulatory	Public	e.g. by law and rule	AU	
	Private	e.g. by law and rule	GU	
Financial	Public	e.g. by category (by vendor)	AU	
	Private	e.g. by category( by vendor)	GM	
HR/Personnel	Public	e.g. by category (working hours, schedules, overtime, )	AU	
	Private	e.g. by individual employee, by category	GM	

Public Relations		by category, matter, company	AU	Documents and Presentations used for public education, advertising, promotion etc. These could be PowerPoint, PDF, Word or other formats
Planning/Budgeting		by year by category	GU	Documents related to planning for the future or budgeting issues
Training	Courses	by course, by topic	AU	Documents related to staff training and staff education
	Conferences/Seminars	by conference, by topic	AU	Documents related to conferences, seminars etc.