QATAR
NATIONAL PROJECT MANAGEMENT

Document Management Plan Preparation Guidelines

TABLE OF CONTENTS

1. Purpose of Document

Note: This document does not cover all the elements of Configuration Management required for technology projects. Note also that it does not describe or assume use of document management software.

Instruction:
This section provides the purpose of the document.

Recommended text:

The purpose of this document is to outline the document management approach for **<insert name of project>** It provides standard terminology, clear roles and responsibilities, and a detailed description of expectations of team members regarding document control. It is designed to guide the project team.

2. Definition of Document Management

Recommended Text:

Documents refer to all project records and deliverables. Document management is the process of organizing, storing, protecting, and sharing documents.

3. Objectives of Document Management

Recommended Text:

The overall goal of document management is to protect a project from losing track of its work or losing the work itself.

Document management achieves this overall goal through the following objectives:

- Provide safe storage and backup of all documents in a project library.
- Provide clarity regarding which version of a deliverable is the latest version.
- Provide a clear record of approved deliverables over the life of the project.
- Provide measures to maintain restricted access to confidential documents.
- Provide an accurate and complete archive of project documents to the permanent organization at the end of the project.

4. Terms, Acronyms and Abbreviations

Recommended Text:

All terms, acronyms, and abbreviations used in this document are defined in the Project Management Glossary at www.qnpm.gov.qa.

5. Document Management Methods

Recommended Text:

This section describes the methods used to control project documents. These include templates, naming conventions, storage, recovery and backup, security, destruction, and approval.

Tips:

Remember that once a Plan is approved, the project must undertake the document management process and methods described in this document. The Project Manager should be held accountable for completing activities described in this Plan by the Sponsor.

This document should describe the nature and extent of document management activities for a specific project. Avoid providing general descriptions of document management best practice.

5.1 Document Templates

Recommended Text:

What follows is a listing of document templates team members are expected to use and a description of the key elements of deliverable templates for document control purposes.

5.1.1 Listing of Templates

Recommended Text:

What follows is a listing of templates and the software and version they use. All team members are expected to use these templates to promote consistency in how team members present work to each other and to the outside world. Team members are also expected to use the software versions listed below to avoid problems sharing documents with other team members.

All templates are provided on a CDROM to team members at orientation, and copies are available to team members on the project server.

Example table for listing templates:

Template Name	Description	Software and Version
Presentations	A standard document for preparing presentations	PowerPoint **<insert version>**
Deliverable Documents	A standard document for preparing written deliverables such as plans and reports	Word **<insert version>**
Meeting Agenda	A format for presenting meeting agendas	Word **<insert version>**
Meeting Minutes	A format for presenting meeting minutes	Word **<insert version>**
Status Report	A format for each team to report status to the Project Manager	Word **<insert version>**
Schedule	The expected format for schedules, including guidelines for level of detail and organization of work packages	QNPM Tool (Primavera) **<insert version>**

5.1.2 Key Components of Templates

Recommended Text:

Key elements of templates for document control purposes are as follows:

Element	Description	Location
Document Status	Two types: Draft: Under development or revision Final: Approved	Front page
Confidentiality Level	Three types: Confidential: restricted circulation Internal: circulation within project Public: no restrictions on circulation	Front page and footer
Copyright	Standard language regarding ownership of material	First page
Authors	Listing of contributing authors and contact information	Document control page after title page
Version History	Listing of version numbers and who was involved in creating each version	Document control page after title page

Element	Description	Location
Approvals	Record of the approved version with signature	Document control page after title page

5.1.3 Document Naming Conventions

Example naming convention:

The standard format for a document file name is as follows:

<Document Status>_<Deliverable Name>_<Document Version Number>_initials of author or revisor>

Example:

Draft Document Management Plan_v2_ML

Final _Strategic Plan_v7_KA

Note: The example above is a straightforward naming convention. Some projects may choose to specify naming conventions for different types of documents and apply a numbering system to deliverables with unique identifiers.

5.2 Document Storage

Tips:

This section outlines where and how documents will be stored. Team members should not store work on their desktops, laptops, or other computers for long periods of time as this makes work vulnerable to loss from accidents, viruses, and employee turnover.

Items to consider when writing this section are as follows:

- How frequently should team members put copies of their work in a safe storage place?
- Are all team members in one location? If no, how will team members working on the same deliverable store and share versions?
- Which team members should have access to which files?
- Will the library be electronic only, or will a hard copy library also be created?
- How should the project file directory be organized? By team? By deliverable?

Example section:

All team members are expected to put electronic copies of their work in the project directory on the project server at the end of each working week using the document naming conventions provided above. A directory has been established on the project server, and team members have limited access to different files on this server based on their role.

Team members are also expected to provide hardcopies of approved deliverables with signatures to the Project Manager for inclusion in a central hardcopy library.

5.3 Document Recovery and Backup

Recommended Text:

The purpose of backup is to allow recovery after a mishap. The first stage of the recovery process must be the analysis of what needs to be restored. Once the extent of what needs to be restored has been determined, recovery action can commence by loading the last full weekly backup followed by the last incremental backup.

Tip:

For important and time critical data, a mirror system, or at least a mirror disk may needed for a quick recovery.

Example section:

This section outlines the recommended document backup and recovery procedure for documents.

Backups should conform to the following best practice procedures:

- All files must be adequately and systematically backed up including updates.
- Records of what is backed up and to where must be maintained.
- The backup media must be precisely labelled, and accurate records must be maintained of those backups completed.
- Copies of the backup media, together with the backup record, should be stored safely in a remote location.
- Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency.

Type	Description	Frequency	Storage Location
Remote Backup	As the name implies, the full monthly backup takes a copy of all files, libraries, and data. The size of a full backup can be large, and the time it takes to complete could impact service availability if not carefully planned.	Monthly	Remote secure location
Full Backup	As the name implies, the full backup takes a copy of all files, libraries, and data.	Weekly	Firebox (Local)
Incremental	The incremental backup uses the Full Backup as a starting point and makes backup copies of data that has changed since the previous backup was taken. In most cases the use of incremental backups radically reduces the time taken to do the backups. It may require some backup management software	Daily	Firebox (Local)

5.4 Document Security

Recommended Text:

This section outlines procedures for keeping documents secure for **<insert project name>.**

The requirements for documents security varies depending on the scale, the sensitivity or importance of the information and activities supported. However the security measures outlined below should be followed:

5.4.1 Confidentiality

Document authors are responsible for setting the level of document confidentiality based on guidelines provided by the Project Manager.

The levels are as follows:

- Confidential: restricted circulation
- Internal: circulation within project
- Public: no restrictions on circulation

5.4.2 Clear Desk Policy

All document users should adopt a “Clear Desk Policy” for confidential and sensitive papers, electronic storage media and other assets to reduce the risk of unauthorised access, theft or damage outside normal working hours.

Where appropriate the following should be considered:

- Sensitive and confidential documents should be locked in cabinets when not in use.
- Sensitive information, laptops, personal digital assistants, and other valuable items should be locked away when not in use.
- All documents should be stored on the central storage device (server).

5.4.3 Removal of Documents

Sensitive and confidential documents on any form of electronic media must not be taken off-site without appropriate authorisation from the information owner or systems owner.

Authorization should only be provided to staff with remote access and staff with permission to work from home.

5.4.4 Equipment Security Guidelines

Equipment should be physically protected from security threats and environmental hazards to both reduce the risk of unauthorised access to data and to safeguard against loss or damage.

The following checklist may be used to identify potential hazards;

- Fire
- Smoke
- Water and other liquids
- Dust
- Vibration
- Chemical effects
- Electrical supply interference
- Electromagnetic radiation
- Theft
- Smoking, eating and drinking should be prohibited in computer areas

5.4.5 Virus Controls

Virus detection and prevention measures and appropriate user awareness procedures should be implemented. Users should be reminded that prevention is far better than cure. The basis of protection against viruses should be founded on good security awareness, appropriate system access controls, and the following specific guidelines:

- Virus-specific detection software (which must be regularly updated and used as directed by the supplier) should be used to scan computers and media for known viruses as a precautionary measure and on a routine basis.
- Change detection software should be installed on computers, where appropriate, to detect any change in executable code.
- Virus “repair” software should be used with caution, and only in cases where virus characteristics are fully understood and the correct repair is certain.
- Any diskettes or CDs of uncertain or unauthorized origin should be checked for viruses before use.

5.5 Document and Media Destruction

Recommended Text:

All documents containing information that has been classified as “confidential” or “internal” by their authors or the Project Manager must be shredded (using a shredder) prior to being discarded.

Any computer hard drive or removable magnetic medium, such as a diskette, magnetic tape, Zip disk, etc., that has been used to hold any kind of “confidential” or “internal ” information must be electronically “scrubbed” prior to being discarded or being transferred to any individual or entity who is not authorized to view such information. On such media, the mere deletion of confidential data is not sufficient as deleted information is still accessible to individuals possessing a number of software tools. Any non-erasable medium, such as a CD, optical disk, etc., that has been used to hold any kind of “confidential” or “internal” information must be physically destroyed before being discarded.

5.6 Document Approval

Recommended Text:

All documents requiring Sponsor approval must go through a compliance review and technical review by the Project Manager before going to the Project Sponsor for review. The compliance review checks whether or not the document complies with the template and matches the deliverable description provided in the Project Plan. The technical review involves the Project Manager reviewing the content for quality.

Once necessary changes arising from the compliance and technical review are made, the Project Manager provides the document to the Sponsor for review and approval.

The Project Manager's compliance and technical review should be completed in five business days. Sponsor approval is expected to take ten business days.

6. ROLES AND RESPONSIBILITIES

Recommended Text:

This section outlines roles and responsibilities for everyone involved in the document management process. This section should only include document management-related responsibilities, and it should contain more detail on document management responsibilities than provided in the Project Plan.

The table below describes roles and responsibilities related to the risk management process.

APPENDIX A: DOCUMENT CONTROL SHEET

Recommended Text:

All project deliverables will have a document control sheet at the beginning to help track versions and approvals. This control sheet lists authors, version history, and approvals as listed below.

AUTHORS

This document was prepared by:

VERSION HISTORY

Date	Document Version	Document Revision History	Document Author / Reviser

APPROVALS

Date	Document Version	Approver Name and Title	Approver Signature