Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

Data Sharing Standard Operating Procedure

Ministry of Information Technology & Telecommunication
DIGITAL PAKISTAN

Document Control

Prepared / Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval
			MOITT	**1.0**	

Change History

SN	Version	Changes Description
1	**1.0**	**Final Version**

Table of Contents

1 Abbreviations

BCP: Business Continuity Plan

SLA: Service Level Agreements

P2P: Peer to Peer

2 Overview

Corporate Information and data are often an organization's most valuable asset. It is very important that information is secured with a high degree of confidentiality, integrity, and availability.

3 Scope

This policy applies to the all employees, contractors and partners who are in the role of the owner, user or custodian of any kind of information assets or in any support role for information handling.

4 Policy

1. Access to information should be granted only on a need to know basis by the information owner.

2. Information owners are responsible for storing any information intended to be protected in an authentication protected storage area.

3. Users intending to share any information for viewing only must take appropriate technological steps to deny modification of that information e.g., by providing read-only access to user. IT Support can be contacted for guidance.

4. Users must not release their password or other methods of authentication (i.e., keys, access cards, etc.) to other users who are not specifically authorized to receive such access.

5. P2P file sharing applications are strictly prohibited on all systems on the network.

6. Folder sharing over the network is prohibited. In event of an unavoidable situation, IT Support should be requested for provision of folder sharing rights over the network. A valid business justification with the approval of Head of IT Department will be required for gaining folder sharing rights.

7. Information to be shared with a group of users should be placed in the protected storage area meant for sharing purposes and grants access only to the authorized users.

8. It is the responsibility of the data owner to provide a list of authorized users of the data being shared to the custodian with the minimum required level of data access permissions.

5 Data Classification

The data being shared must be classified before being shared to other network user(s). The following definitions shall be used to classify data for security purposes:

PUBLIC (OPEN): Information that will not result in any damage if it becomes generally known. Information in the public domain that have been approved for public use by the information owner.

OPEN documents do not need to be labelled. Labelling is at the discretion of the owner of the information.

RESTRICTED (INTERNAL): Information that can be freely shared among employees, but is not approved for general circulation outside the organization where its disclosure would inconvenience the organization or management, and may lead to financial damage or loss of reputation for the organization, or have negative effects for certain customers.

Labelling is the responsibility of the owner of the information. Labelling shall be with the words "INTERNAL".

CONFIDENTIAL: Information which is considered critical to the organization's on-going operations and which can be shared internally in the organization on a need-to-know basis. If unauthorized people gain access to CONFIDENTIAL information, this may lead to significant financial damage or significant loss of reputation for the organization, or have considerable negative effects for certain customers.

Labelling is at the responsibility of the owner of the information. Labelling shall be with the words "CONFIDENTIAL".

SECRET: Highly sensitive internal documents. If unauthorized people gain access to SECRET information this may lead to very serious financial damage or loss of reputation for the organization or may have very serious negative effects for certain customers. Security at this level is the highest possible.

Labelling is the responsibility of the owner and senior management. Labelling shall be with the words "SECRET".

For further information on classification please see Data Information Classification

6 Data Handling

Data handling requirements may vary depending on the classification of data shared. However, it is anticipated that most data shared will involve a mix of data classes including CONFIDENTIAL and possibly SECRET information. Therefore, whenever data elements are aggregated for collection, transmission, or storage, the aggregate data shall be handled using the Data Handling Standard that apply to the most sensitive data element.

7 Policy Exception

It is imperative that all employees comply with all Information Security Management System policies. However, there are circumstances that fall outside the ability to comply with and/or conform to a policy. In such instances, an exception must be documented and approved. This defines the requirements to formally authorize exceptions where control cost is much greater than the risk represented from non-compliance to policies/SOPs.

Requests for exception must include:

a. A valid business justification

b. A risk analysis, compensating controls to manage risk, and technical reasons for the exception.

Requests for exception that create significant risks without compensating controls will not be approved. Requests for exceptions must be periodically reviewed to ensure that assumptions or business conditions have not changed.

References:

ISO 27001
• **A.13.2.1 Information Exchange Policies and Procedures** • **A.13.2.2 Exchange Agreements**