Information Technology Security Policy related to the Accounting/Financial Data of Punjab State Road Sector Project

Security can be defined as "the state of being free from unacceptable risk". The risk concerns the following categories of losses:

- Confidentiality of Information.
- Integrity of data.
- Efficient and Appropriate Use.
- System Availability.

This policy shall be effective from the date of approval of the same from the World Bank & applies to PRBDB with its implementing divisions of Punjab Sate Road Sector Project and issued under the authority of Mr. M.S. Nijjar (Project Director). PRBDB as well as its implementing units must apply this policy to meet their information security needs. Instances of non-compliance must be reviewed and approved by the authorized person of the concerned department.

PURPOSE OF THIS POLICY

By information security we mean protection of the accounting data, accounting software, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security policy is to protect accounting/financial data which contains all accounting/financial information related to the project.

RESPONSIBILITY

At the implementing division: Executive Engineer of the division shall be responsible for establishing procedures to implement the policy & for monitoring compliance of the same.

At the PRBDB: Controller Finance shall be responsible for establishing procedures to implement the policy & for monitoring compliance of the same.

Responsible person should see to it that:

- The compliance of the information security policy shall be monitored on a regular basis and disclosed as appropriate.
- Appropriate training is provided to data owners, data custodians, network and system administrators, and users.

Accounting/Financial Data Security Policy:

- **Authorized Access & the Password**: Systems that contain accounting /financial data must be password protected. At the divisional level only the concerned Executive Engineer, Accounts Officer & tally operators shall be authorized to access the accounting software. In case of PRBDB the Project Director, Controller Finance, the Manager Accounts & the tally operator shall have the access to the system. The password should be checked on regular basis. In case, any of the above authorized person leave the office due to transfer, retirement etc. then the password must be changed with immediate effect.

- **Back-Up:** Back Up of the data should be taken on regular basis. For the purpose of the back up, tally operators may be provided the pen drives & these shall remain in the custody of the Accounts officer. Besides taking the back up of the data in the external storage device, a copy of the same may also be maintained in the local hard disk or the server by making a back up directory.

- **Locking of the back dated vouchers**: Entries of back dated vouchers shall be discouraged. Accounting Entries shall be locked automatically within 10 days of the making the entry in the accounting software tally at all the divisions. In the exceptional circumstances like any tally operator left the office, Executive Engineer shall have the power to open the back lock.

- **Hard Copies of the Day Book, Ledgers & Trial Balances**: The print outs of the day book & ledgers shall be taken on the weekly basis & shall be duly signed by the accounts officer & the Executive Engineer at the divisions. In case of PRBDB, the print outs of the same shall be signed by the Controller Finance. Hard Copies of the Trial Balance shall be taken on Monthly basis & signed by the Executive Engineer of the divisions. The same signed copy of the Trial Balance shall be sent to the PRBDB for the consolidation of the accounts. After the consolidation of the accounts, monthly consolidated hard copy of the Monthly Trial Balance shall be signed by the Controller Finance. A separate file for each division & PRBDB

shall be maintained at PRBDB for the record keeping of the Monthly Trial Balances.

- **Virus Prevention**: The desktop systems, Servers & Work Stations that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.

Compliance Reporting:

- Compliance report, certifying that

  (i)The password has not been shared with any unauthorized person,

  (ii)Access to the system containing financial software has only been made by the authorized person,

  (iii) The back dated vouchers have been locked as per the policy,

shall be submitted by the divisions to the Controller Finance of the PRBDB. Further the consolidated compliance report of the PRBDB including the compliance reports of the divisions shall be submitted to the Project Director on the monthly basis.