Kuwait Finance House بيت التمويل الكويتي **Reference Number** **RMD/IM-293/15-2015**	**RISK MANAGEMENT DIVISION** **CIRCULAR MEMORANDUM**

Date : 17 August 2015

To : All KFH Malaysia Employees

From : Mr. Ahmed S Al Kharji, Chief Executive Officer & Managing Director

Cc : Nora Shah Abdul Wahab Shah, Chief Corporate Affairs
Mohd Zaki Abdullan, Chief Internal Auditor

Re : Protection of Data and Utilisation of Assets

1. Objective

The objective of this Circular Memorandum is to notify all employees on the new policies regarding the protection of data and utilisation of assets.

2. Background

Providing protection and ensuring proper utilisation of the Bank's data and assets has always been and shall continue to be a vital concern of the Bank. Various policies and procedures on protection of data and management of the Bank's assets had been established and implemented accordingly.

In order to further improve the existing policies and procedures, the Board of Directors and Senior Management has taken a pro-active action in implementing Data Loss Prevention (DLP) System for the Bank. As at to-date, the implementation of DLP System has reached its final stage and upon completion of this project, the system will be managed by Risk Management Division with support from IT team.

The DLP system is able to monitor the movement of the Bank's data via various channels such as network and endpoint (e,g, USB, external drive, printer), and safekeeping of documents in the Bank's computer system by unauthorised parties. In addition to the above, in order to ensure the Bank's data is not accessible to unauthorised parties, it has been decided that the Bank's notebooks must be encrypted and mobile devices belonging to the employees who have the access to the corporate email must be installed with DLP agent.

3. New Policies for Observation

i) Encryption of Bank's Notebooks

All the notebooks given to the employees must be encrypted. This exercise will be done in stages and the respective staff will be informed to back-up their data in the shared folder and surrender their notebooks for encryption to Risk Management Team. The time required to install the

encryption agent for each notebook is approximately 15 minutes. Access to the encrypted notebook is via User ID and Password of the respective employee. Once encrypted, the information kept in the notebook will not be accessible to unauthorised parties unless the Password is compromised. All employees are reminded that sharing of User ID and Password of the encrypted notebook is STRICTLY PROHIBITED.

ii) Transfer of Data to USB and External Drives

Currently, the Bank has blocked the access to USB and external drives for all computers except for those with prior notification to the Board of Directors. Transfer of data from the Bank's computer to the USB and other external drives is prohibited even in the event if the access is temporarily opened (due to intermittent system issue or trouble shooting). Request for access to the USB and external drives will only be given due to critical job requirement and must be recommended by the respective Chief of Division and subsequently concurred and approved by the Chief Risk Officer.

iii) Sending of Bank's Data to Personal Email

From the review of the alerts generated by the DLP System, it was found that there were many instances where employees were sending emails containing either the Bank's data and/or personal data to their own personal email address. The Bank has decided that due to the need to protect the Bank's data from being intercepted and accessible by unauthorised parties, either through public email or one's own personal computer, all employees who plan to do their office work at home are required to bring back their notebook (for the notebook users) or to come to office. The sending of any Bank's data by staff to their personal email is STRICTLY PROHIBITED and we would like to reiterate that the email transactions performed by all employees are currently being monitored by the DLP system.

Kindly take note that the Bank's email system should be used for official business matters only. The above policies shall take effect immediately and disciplinary action/s may be taken against employees who fail to comply with the policies.

Please be guided accordingly.

Thank you.

KEN YON
Chief Risk Officer

AHMED S AL KHARJI
Chief Executive Officer & Managing Director