Kuwait Finance House
بيت التمويل الكويتي

OPERATIONAL RISK MANAGEMENT
Data Loss Prevention (DLP) Governance Policy

Establishment Date : September 2015
Implementation Date : September 2015
Revision Number : 0
Policy Registration Number: RMD/ORGMR/POL/2015/004/DLP

Task	Signature	Name	Department/ Division/ Committee	Date
Prepared By		Kalsum Hassan	Risk Management	11 Aug 2015
Reviewed By		Ken Yon	Risk Management	11/8/15
Reviewed By		Aminuddin Abu Bakar	Shariah	11/8/15
Reviewed By		Mohd Zaki Abdullah	Internal Audit	4/8/15
Recommended By		Management Committee		27/8/2015
Noted By		Board Audit Committee		9/9/2015
Concurred By		Board Risk Management Committee		9/9/2015
Approved By		Board of Directors		10/9/2015

DOCUMENT HISTORY

Establishment Month	Approval Date	Version	Author	Remark
May 2015		00	Securepath	Draft
June 2015		00	Kalsum	

TABLE OF CONTENTS

1.0 INTRODUCTION

Kuwait Finance House (M) Bhd (the Bank or KFH Malaysia) Data Loss Prevention (DLP) Governance policy is aimed to monitor the potentially sensitive/confidential information leaving the Bank environment in violation of KFH Malaysia's Security Policy. This DLP Governance Policy is intended to act as a guideline for the Bank to implement DLP system.

This Policy compliment the Bank's overall risk management process in managing and protecting the Bank's data and applicable to all divisions within the Bank. Generally, the Policy covers electronically stored information. The DLP system is implemented in the Bank's infrastructure with the purpose to provide appropriate protection on the use of Bank's information, device and technology in the course of conducting business. The main function of the DLP system is to detect, alert and block potentially confidential/sensitive information leaving the Bank. All the employees are subject to DLP system monitoring.

The Bank's DLP system implementation covers Data in Use, Data in Motion and Data at Rest.

2.0 OBJECTIVES

The objectives of the Policy are to:

I) Provide a comprehensive and sound framework for data loss prevention implementation.

II) Ensure that the Bank's information is only accessible and release to the authorized party.

III) Ensure that there is clear assignment of roles and responsibilities for data management within the Bank.

IV) Provide guidance on the process for monitoring, reporting and reviewing the DLP incidents.

V) Ensure that control measures are in place to safeguard the Bank's data.

VI) Provide guidance on the recommended business policy or rules.

VII) Ensure there is regular awareness campaigns to refresh the employees understanding on the data protection and policy.

3.0 COMPLIANCE AND CROSS REFERENCE

I) Data Management and MIS Framework (BCOS/ITD/POL/227/13/DMMF)
II) General Systems Security/Controls on ID and Password Policy (QMS/ITD/POL/45/05/GSSC)POL/235/13/IC)
III) Information Classification Policy (BCOS/ITD
IV) Discipline Policy (QMS/HRA/POL/19/05/DISP)
V) Code of Ethics (QMS/HRA/POL/19/05/DISP)
VI) BNM Guidelines on Data Management and MIS Framework
VII) Islamic Finance Services Act 2013
VIII) Personal Data Protection Act 2010

4.0 ABBREVIATION AND ACRONYMS DEFINITION

DLP	Data Loss Prevention
IAD	Internal Audit Division
IT	Information Technology
KFH Malaysia/Bank	Kuwait Finance House (Malaysia) Berhad
MANCO	Management Committee
RMD	Risk Management Division

5.0 SCOPE

This Policy is prepared by Risk Management Department and it shall be reviewed every 2 years. The Policy is by no means exhaustive, and it is not intended to cover all situations that may occur. However, its principles, standards and process should be used as guidance.

All employees are required to ensure compliance with the requirement stated in this Policy. All deviations to this Policy must have an action plan and time frame for compliance.

The scope of the Policy covers the Data in Use, Data in Motion and Data in Rest. In addition it also covers the encryption of hard disk of the Bank's notebooks provided to the employees and mobile devices (only for employees that are given access to the Bank's email network via mobile devices).

6.0 DEFINITION

I) Data in Use

Data in Use refers to data that is not passively stored in a stable location such as central data folder/server but is working its way through other parts of IT infrastructure. Data in Use may be in the process of being generated, amended or updated, erased or viewed through various interface endpoints. This is an active data currently process by the system application.

II) Data in Motion

Data in Motion also known as data in transit. It refers to information that is moving through a network. For example, when sending an email, that email is defined as Data in Motion, i.e. between the time when the email was sent and the time when it actually reaches the recipient's email host.

III) Data at Rest

Data at Rest is referring to inactive data which is stored in any digital form. It includes all data in storage such as archived, data which is not being assessed or changed frequently, files stored on hard drives, USB drives, back-up tapes and disks, etc but excludes any data that frequently traverses the network or resides in temporary memory.

IV) Information or data

Includes electronically stored, non-public, proprietary, confidential, sensitive data, facts, processes, procedures or other material owned by the Bank.

V) Devices

Includes electronic equipment (such as computers, mobile phones, PDAs, etc) or storage media (such as USB, CDs, DVDs, iPods, etc) with the capability to store information.

VI) Technology

Computer programs or systems used to access, transmit, store or exchange information.

VIII) Data Steward

The Data Steward is a representative of the respective Division/Department who is responsible to liaise with the DLP Core Team to review the alerts generated by the DLP System.

IX) DLP Core Team

The party responsible handling the DLP system, policy and process for the Bank. Currently, the DLP Core function resides with the Operational Risk Management team of RMD.

X) DLP Data Owner

The party responsible in generating the data, ensuring its accuracy, integrity and timeliness. In this document the Data Owner is referring to the Chief of Division.

7.0 DATA LOSS PREVENTION PROCESS

I) DLP System Monitoring Function

a) Outbound Emails and Web Channel

DLP system monitors the Bank's outbound emails and web channel. Only outbound emails shall be monitored for violations of DLP business rules.

The DLP system has the capability to monitor and track the emails sent out from the Bank's environment. If the respective emails violate any of the business rules, alerts will be generated by the DLP system for monitoring by the DLP Core Team.

Only authorized staff (due to operational requirement) is allowed to upload data to approved web channels. Approval for authority to upload to web channels must be properly justified and approved by the respective Chief of Division.

b) Monitoring of Users Machines

The DLP system monitors the computer system for any outflow of confidential/sensitive data through channels such as external USB devices, printers, network shared folders, browsers, CD/DVD and email client software.

When confidential/sensitive data is found being transmitted out (either via email/web channels/external USB drives/CD/DVD/etc), the DLP system shall generate alerts for DLP Core Team review.

The access to external disk, USB devices and CD/DVD is only allowed to authorized users. All request for access to external disk, USB devices and CD/DVD must be recommended by the Chief of Division and approved by the Chief Risk Officer. The Chief Internal Auditor will be notified on any access given.

c) Folders of the Personal Computers

All folders shall be enforced with proper access control to limit access to authorized parties only. The DLP system may be configured to scan the folders of the Personal Computers for confidential/sensitive data that is inappropriately stored. If confidential/sensitive data is found in an unauthorized location, DLP alerts shall be generated for further review and subsequent action by the DLP Core Team. This function is to be used only upon obtained approval from the Chief Executive Officer or the Board Audit Committee.

II) DLP Business Rules

The DLP business rules are developed according to the specific business process. Each data owner (division) needs to identify and classify his data according to the Bank's classification policy. Each business rules should be unique and is created for the specific confidential/sensitive documents or information. The data owners are responsible to identify their own business rules. These business rules will be uploaded into the DLP system for monitoring of possible data leakage.

The request for new/amend/delete the DLP Business Rules must be recommended/ concurred by DLP Core Team and approved by the Chief Risk Officer. Notification on the new/amendment/deletion of the DLP Business Rules is to be submitted to the Administrative and Operations Committee for notification.

III) DLP Alerts

DLP system shall generate alerts centrally for review. The alerts will be generated by the DLP system if the transaction performed hits any business rules uploaded into the system. The responsibility to review/monitor the alerts is under the purview of the DLP Core Team. The DLP Core Team together with the Data Steward will conduct the first level review of the incident, evaluate the sensitivity of the data and determine whether its transfer is authorized.

Each member of DLP Core Team is not allowed to review the alerts resulting from the transaction performed by him/herself. The Chief Internal Auditor is responsible to review alerts for the transaction performed by the Chief Risk Officer only.

Only the Chief Risk Officer has the authority to review the alerts generated from the transactions performed by the Members of the Board of Directors, Senior Management (except for the transaction performed by the Chief Executive Officer) or identified critical functions. In the absence of the Chief Risk Officer, this function shall be taken over by the Chief Internal Auditor. The access to view the alerts arising from the transactions executed by the Chief Executive Officer is only given to the Chairman of the Board Audit Committee or Board of Directors.

The Chief Executive Officer has the authority to view the alerts for the transactions executed by all parties.

Access to the DLP alerts is restricted to the DLP Core Team and the corresponding Data Steward to protect the privacy of the Bank's data. A DLP alerts does not constitute evidence that an employee has intentionally or accidently lost data but it provides sufficient basis for review and investigation to determine whether data has been inappropriately used or transferred.

IV) Investigation of DLP Incident

If there is any confirmed unauthorized or inappropriate use of Bank's data detected, the DLP Core Team shall notify the respective Chief of Division and Chief Executive Officer (except for the case involving the Chief Executive Officer). If in-depth investigation is warranted, the details of the incident will be forwarded to the Chief Internal Auditor. For incident involving the Chief Executive Officer, the Chief Internal Auditor is to notify the matter to the Chairman of Board Audit Committee the soonest the incident was discovered.

The outcome of the investigation is to be presented to the Chief Executive Officer (except for the case involving the Chief Executive Officer) and Board Audit Committee for decision.

If there is any violation of policy incident involving the Chief Internal Auditor, the Chief Risk Officer is to forward the matter directly to the Chief Executive Officer. The Chief

Executive Officer is empowered to decide on the investigating party for cases involving the Chief Internal Auditor.

Disciplinary action may be taken against the respective employee if the investigation revealed intentional leakage of Bank's data to unauthorized party.

8.0 ROLES AND RESPONSIBILITIES

I) DLP Data Owner

The DLP Data Owner is responsible for the following actions:

a) Overall stakeholder of the data under his/her jurisdiction.

b) Ensure all the confidential/sensitive data is properly classified in accordance to the Bank's Data Classification Policy and being indexed by the DLP system.

c) Validating the alerts generated by the DLP System.

d) Give full cooperation to the DLP Core Team and Internal Auditor during review and investigation of DLP alerts.

e) Recommend any new/amendment/deletion of DLP business rules to DLP Core Team.

II) DLP Data Steward

The DLP Data Steward is responsible for the following actions:

a) Owning the DLP alerts relating to his/her division.

b) Ensure that the confidential/sensitive data is being communicated to the DLP Core Team for indexing by the DLP system.

c) Review the new/amendment/deletion of the business rules for recommendation to the DLP Data Owner and subsequently to the DLP Core Team.

III) DLP Core Team

The DLP Core Team is responsible for the following actions:

a) Monitoring, prioritization, review, investigation and escalation of DLP alerts generated by the DLP system.

b) Reviewing the DLP business rules submitted by the Data Owners for presentation to Administrative and Operations Committee for approval.

c) Upload the new approved DLP Business Rules into the system.

d) Implementing and supporting the DLP system configurations.

e) Escalate to Vendor or IT Team whenever there is any problem noted in DLP system.

IV) Internal Auditor

The Internal Auditor is responsible for the following actions:

a) Investigation of DLP alerts escalated by DLP Core Team.

b) Escalation of confirmed violation of DLP Policy incident to the Human Capital Division, Chief Executive Officer or Chairman of Board Audit Committee and Board Audit Committee.

The Chief Internal Auditor is responsible for the following actions:

a) Review the alerts from the transactions executed by the Chief Risk Officer.

b) In the absence of the Chief Risk Officer, the Chief Internal Auditor is to review the alerts for the transactions performed by the Members of the Board, Senior Management and other identified critical function.

Disciplinary action may be taken against staff who had negligently or intentionally release the Bank's data to unauthorized party or found guilty in using the Bank's asset for personal usage.

V) Board Audit Committee

The Board Audit Committee is responsible in deliberating and providing the decision on the investigation on DLP policy violation performed by the Internal Auditor.

9.0 DLP INCIDENT HANDLING

In the event that one or more of the DLP Business Rules are breached by the activities done by the employees, DLP alerts will be generated by the DLP system. The DLP Core Team will assess the alerts which may lead to the below outcomes:

I) False Positive

The DLP system may generate false positive alerts due to limitation of signature based pattern matching or DLP business rules uploaded are too general. Hence, upon review of such alerts, the DLP Core Team may indicate those alert as false positive.

If it is possible to adjust the DLP business rules to avoid similar false positives in the future, the DLP Core Team together with the respective Data Steward and Data Owner will perform the fine-tuning. All the fine-tuning must be approved by the Chief Risk Officer and notified to the Administrative and Operations Committee.

II) Policy Violation

DLP system will detect users committing policy violations. For example, when the users copy the confidential information to a USB drive or send the confidential information to external email address. The DLP Core Team together with the corresponding Data Steward will review all the alert generated to confirm whether it is an actual violation. If the DLP Core Team has a strong basis to suspect the incident as a potential violation, the matter will be escalated to Chief Executive Officer for notification and Internal Audit Division if in-depth investigation is warranted.

10.0 ENCRYPTION OF BANK'S NOTEBOOKS

All the Bank's notebooks must be encrypted before it is being handed over to the employees for usage. The encryption of the hard disk of the notebooks is done in order to protect the data kept in the notebooks in the event of missing of notebooks or notebooks being accessible to unauthorized party. When the hard disk of the notebook is encrypted, only authorized parties are able to access to the information kept in the notebook.

The file copied to the external drives, USB devices and CD/DVD from the encrypted notebook will also be encrypted automatically. The request to temporarily decrypt the notebooks and all external devices will only be given due to critical job requirement and must be approved by the Chief Risk Officer or his delegates.

Any changes to the approved encryption rules must be recommended by the Chief Risk Officer, and approve by the Administrative and Operations Committee.

Refer to Appendix A for the list of the Endpoints Encryption Rules Settings implemented by the Bank. The rules is in-line with the Bank's General Systems Security/ Controls on ID and Password Policy.

11.0 MOBILITY SUITE FOR MOBILE DEVICES

The access to the Bank's corporate email via the employees' personal mobile devices will only be allowed due to operational requirements. All the requests made must be approved by the respective Chief of Division.

All the mobile devices must be installed with DLP mobility agent prior to access to the Bank's corporate email is allowed irrespective whether the access is via personal or Bank's mobile devices. All the Bank's information stored in the mobile devices will be wiped remotely in the event of missing mobile devices, resignation or employee's access to Bank's information is no longer authorised.

The access, security level and usage of the Bank's mobile devices is restricted in accordance to the rules as listed in Appendix B. Any changes to the mobility rules must be approved by the Administrative and Operations Committee.

12.0 EMPLOYEES AWARENESS

I) All employees should report any suspicious or potential incident of leakage of Bank's confidential information to DLP Core Team.

II) All employees are required to comply with the data management and classification policies and security policies set by the Bank and Regulator.

III) All employees must ensure that the Bank's laptop and portable devices such as i-PAD, mobile devices, etc are not left unattended and unsecured.

IV) All employees should not share or reveal their password to another parties.

V) All employees should use strong passwords for the laptops/desktops and application access, in-line with the Bank's security policy on password strength.

VI) The Bank shall regularly conduct relevant awareness campaigns and training to refresh employees understanding on data protection.

VII) All employees are encouraged to practice prudence when handling and sending out sensitive data. Employees are required to check the outgoing mail and its contents to ensure it is being sent to the target audience by verifying the recipient list.

13.0 EXEMPTION TO DLP SYSTEM MONITORING

All employees of the Bank shall be subjected to DLP system monitoring, unless formal approval is granted.

In the event if exception is required due to business requirements, a formal request must be submitted to Management Committee and Board of Directors for approval and notification respectively.

APPENDIX A

Endpoints Encryption Rules Settings

The encryption rules implemented by the Bank is as below:

Management Agent	
Password attempts	After 3 incorrect attempts, pause for 5 minutes between further attempts.
Communication	Send status updates every 60 minutes.

Password Complexity	
Minimum password length	8
Non-alphanumeric characters	!@#$%&*+?<>^()-={}[]|\;:’”/,.

Drive Encryption	
Client administrator	IT Team
Authentication method	Require registered users to authenticate with a password
Single sign-on	Enable
Self-recovery	Disable
Preboot log-in screen	Custom KFH Malaysia logo
Log-on message (80 characters)	The usage of this PC is subject to the Bank’s DLP Governance Policy
Text colour	White
Prefill the log-on form with the most recent	User name Domain
AES encryption strength	256 bit
Disk drives	Encrypt all disks
Client monitor	Lock computer after 30 days without contact Warn users 10 days before locking computer

Drive Encryption	
Help desk recovery	Enable Helpdesk recovery Helpdesk recovery communication unlock
Self-encrypting drives	Enable hardware encryption for compatible Opal-compliant drives http:/www.symantec.com/docs/TECH226779
Access	Allow read and write access to files on removable media
Encryption format	SEE RME (Symantec Endpoint Encryption Removable Media Encryption)
Automatic encryption	Encrypt new files
On-demand encryption	Users can right click to encrypt existing files on removable media
Exemption for multimedia files	Disabled
File types exclusions	Disabled
Device exclusions	Disabled
Users may encrypt files with	Password
Default password	Password
Session password	Do not allow users to set session password
Device session password	Do not allow users to set a device session password for each removable device
Self-decrypting archive	Disabled
Users can use expired certificates to encrypt files	Disabled

APPENDIX B

Mobility Manager Rules Settings

The mobility manager rules implemented by the Bank is as below:

Password Policy (for Corporate Mobile Devices only)	
Auto-lock	Device automatically lock after 15 minutes
Password	i) Simple password, permits the use of repeating, ascending and descending character sequence ii) Password history – 24 times iii) Password expiration – 90 days iv) Failed attempt – never
At Application Level	As per the Bank's password management (in accordance to the password policy of BNM Guidelines on Management of IT Environment)

Password Policy (for Personal Mobile Devices only)	
Auto-lock	Device automatically lock after 15 minutes
Password	Simple password, permits the use of repeating, ascending and descending character sequence
At Application Level	As per the Bank's password management (in accordance to the password policy of BNM Guidelines on Management of IT Environment)

Device Functionality Restriction Policy (for Corporate Mobile Devices only)	
Application Installation	Disable
Camera	Disable
Explicit Content	Disable music or video content purchase.
Screenshots	Disable
In-Apps Purchases	Disable
Game Centre	Disable
Game Centre Friends	Disable
Multiplayer Gaming	Disable
Activity Continuation	Disable moving of items/tasks from the mobile device to other devices
YouTube	Disable
ITunes Music Store	Disable
Untrusted TLS Prompt	Automatically rejects untrusted HTTPS certificates
iCloud	Disable iCloud backup and sync
Photo Stream	Disable
iBookstore / Erotica	Disable

Work Mail Policy (for Corporate and Personal Mobile Devices)	
My friends Modification	Disable
Pairing and Sharing	All pairing and sharing are disabled
Factory reset	Disable
Own Restriction	Disable
Email	Allow HTML email
Copy contacts and clipboards	Disable
Maximum attachment size	10M
Maximum days to sync	Unlimited
Maximum body size	Unlimited
Calendar sync	Unlimited
Storage card	Allow storage card (with encryption)
Roaming	Manual syncing when roaming

Content Policy (for Corporate and Personal Mobile Devices)	
Offline access	Allow offline access
Sharing	Disable sharing of content with other apps Disable content downloads to a desktop
Poll server	Check for updates every 12 hours
Version updates	Automatically push download of new versions with grace period of 4 hours.

Application Policy (for Corporate and Personal Mobile Devices)	
Authentication	Disable
Document and clipboard sharing	Disable
Browser choice	Destroy data and disable app on jailbroken or rooted devices. Block airdrop, airprint, filesharing on social media, adding files on safari, iTunes sharing and iCloud sharing (for iOS).
If the client or MDM is disabled (for android only)	Block app from running.
Poll server	Automatically connect to server to check for updates every 24 hours.
Upgrade	Force upgrade on new version with grace period of 24 hours.

Compliance Rules Policy (for Corporate and Personal Mobile Devices)
Device not jailbroken/rooted device.
Block access to email through email proxy and wrapped applications.

Compliance Rules Policy
Enable app and device management with wipe (Limited wipe for personal mobile devices).
Enable collection and display of personal identification information.
Request device data for every 1440 minutes