Circular No.: NSDL/POLICY/2014/0093 Date: August 28, 2014

Subject: Specifications for tamper proof of storage of DIS image.

As Participants are aware, SEBI Circular No. CIR/MRD/DP/01/2014 dated January 7, 2014 (*which was attached to the NSDL Circular dated January 8, 2014*) requires depositories to put in place adequate checks and procedures to prevent unauthorized changes to scanned DIS. Accordingly, the guidelines on signing and posting the DIS image and tamper proof storage were issued vide Circular No. NSDL/POLICY/2014/0085 dated August 5, 2014. As mentioned at para 3 (d) of this NSDL Circular dated August 5, 2014, the detailed specifications for tamper proof storage of DIS image are given below:

1. The DIS serial number or any other reference key (*which is mapped to DIS number*) used as index field to access DIS image in storage system or as a file name of the DIS image must be stored in an encrypted form. This will make it difficult for any unauthorized user to locate the DIS image in storage system. The encryption key used for encryption should be stored in a secured manner in storage system and should not be accessible to any unauthorized person.

2. Users of the storage system should have rights on need to know and need to do basis.

3. Storage system must store control information i.e. '*Date*' and '*Count of number of DIS image stored for the date*' separately in encrypted form at all times.

4. Storage system should be designed to only add new records. When an authorized replacement of the original DIS image is required, the original image record for that DIS should only be marked as 'replaced' and must not be physically deleted. Further, new DIS image for the aforesaid DIS will also be stored with the same DIS serial number by incrementing the version number of DIS in file name of scanned image.

5. Storage System should process the response file (i.e. zip file) received from DIVS System. Storage System should have following checks while processing response file:

   (a) DIS serial numbers mentioned in the index files should match with the file name of the DIS images.

(b) Verification of NSDL Signature affixed with each accepted DIS image should be done before storing in the storage system.

6. Backend updates (i.e. through SQL commands) must be strictly discouraged and if it is required to be carried out then the same must be carried out after consulting the vendor. Such activity must be carried out in a controlled environment and system should maintain complete audit trail of date, time of update and pre and post image in a separate text file. Ordinarily User-ID with rights for the backend database updates (i.e. Database Administrator ID) shall be disabled by system administrator, and this should be enabled only on a need basis after due authorization.

7. Any database specific activity like back up of database, reorganization of the database, housekeeping requiring data base administration rights, must be carried out using front end application in the Storage System.

8. Integrity Checks:

(a) Storage system should have integrity check program which can be executed at any point in time as desired. This program shall be executed atleast once in a day, either at the beginning or at the end of the day. This program should generate count of all DIS image records stored and verify the same with the control information stored separately in encrypted form.

(b) Storage System should also have integrity check once a week to identify unauthorized change involving additions/ modifications. This can be done either -

i. by performing verification of NSDL signature associated with each DIS image.

or

ii. any other means involving checksum/ HASH of all the DIS image stored with encryption so that integrity algorithm can generate such checksum / HASH afresh and compare the same with one stored with encryption to detect unauthorized modifications carried out to existing DIS image(s).

(c) An alert should be generated in case of any mismatch found in process (a) and (b) above and should be recorded in exception table in the system. Participant should

monitor the alert(s) thus generated, take corrective action and report the same to NSDL.

(d) Internal / Concurrent auditor is also required to check the alert(s) generated during the audit period and report the same in the audit report.

For and on behalf of
National Securities Depository Limited

Samar Banwat
Senior Vice President

FORTHCOMING COMPLIANCE			
Particulars	**Deadline**	**Manner of sending**	**Reference**
Investor Grievance Report (Monthly)	By 10th of the following month.	By email at dp_igreport@nsdl.co.in Alternatively, by hard copy to the Investor Relationship Cell.	1. Circular No. NSDL/PI/98/500 dated October 6, 1998. 2. Circular No. NSDL/PI/2004/1688 dated September 16, 2004.
Networth Certificate and Audited Financial Statements	September 30th every year.	By hard copy to Participant Interface Department.	Circular No. NSDL/PI/98/414 dated September 1, 1998.

Digitally signed by
Name : Samar Banwat
Date : 8/28/2014 8:34:22 PM
Reason : Authentication