The Information Technology (Controller of Digital Locker) Rules, 2016

In exercise of the powers conferred by clause (x) of sub-section (2) of section 87 read with sections 67C and section 6A of the Information Technology Act, 2000 (21 of 2000), the central Government hereby makes the following rules regulating the applications and other guidelines for DigiLocker service providers, namely:

1. Short Title and Commencement:

(1) These rules may be called the Information Technology (Controller of Digital Locker) Rules, 2016.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions:

(1) In these rules, unless the context otherwise requires, -

a) ñActòmeans the Information Technology Act, 2000 (21 of 2000);

b) ñaccess gatewayò means licensed system to provide access to repositories under Digital Locker System;

c) ñapplication program interface (API)ò means a set of routines, protocols, and tools for building software applications;

d) ñappropriate governmentò means appropriate government as defined in clause (e) of sub-section (1) of section 2 of the Act;

e) ñbody corporateò means any company and includes a firm, Limited Liability Partnership, sole proprietorship or other association of individuals engaged in commercial or professional activities;

f) ñcontroller of digital lockerò means the officer of the Government notified as the Controller of Digital Locker;

g) ñDeitYò means Department of Electronics & Information Technology, Government of India.

h) ñdigital lockerò, means a service of preservation, retention and delivery of electronic records to the user;

i) ñDigiLocker Practise Statementò means a statement by the DigiLocker service provider describing the services and flow of the services being offered by the provider.

j) ñDigiLocker service providerò means an agency including a body corporate or an Agency of the Government, licensed by the Controller of Digital Locker, to establish and manage digital locker system electronically, in accordance with these rules;

k) ñdocument Uniform Resource Identifier (URI)ò, means documents or records issued complying with prescribed technical specifications;

l) ñGovernmentò means the Government of India;

m) ñIssuerò means any department or agency of the appropriate Government issuing digitally signed or equivalently authenticated electronic records to the subscriber under Digital Locker System;

n) ñLicenseò means binding agreement between/among the Controller of Digital Locker and any service provider;

o) ñDigital Locker Portalò means a web and mobile based system to provide access to documents under Digital Locker System;

p) ñNational Digital Locker Portalò means DeitY owned and operated web-based hosting Digital Locker System;

q) ñrepositoryò means an electronic repository of digitally signed as well as digitised electronic records, maintained by any DigiLocker service provider for the purpose of accessing such records and delivering them to the users.

r) ñRequesterò means any department or agency of the appropriate Government requesting access to subscribers digitally signed or equivalently authenticated electronic records preserved and retained in the repository created and managed under Digital Locker System;

s) ñsubscriberò means subscriber to a digital locker under the Digital Locker Portal;

t) ñuserò means a subscriber, issuer or requester of the Digital Locker System.

(2) Words and expressions used and not defined in these rules but defined in the Act and Rules shall have the same meanings assigned to them in the Act and the Rules made thereunder.

3. Digital Locker System:

(1) For the purpose of providing preservation and retention of machine readable, printable, shareable, verifiable and secure appropriate Government and private agency issued electronic records, the Government and other service providers to provide a digital locker system of limited electronic storage to all users.

Explanation. ï It is hereby clarified that the present rules provide for the administration of digital locker system by Controller of Digital Locker through DigiLocker Service Providers in accordance with the technical standards as laid down by controller from time to time.

(2) Subject to the sub-rule (1), the digital locker system shall act as web and mobile based portal, to be a Digital Locker Portal for appropriate Government and private agency issued electronic records maintained in a prescribed format.

4. Operation of Digital Locker System:

(1) Any individual who is resident of India shall be able to open and gain access to digital locker after submitting duly prescribed application form to the Controller of Digital Locker after due authentication manner prescribed by the Controller of Digital Locker.

(2) Subject to the sub-rule (1), citizen may obtain the services of the licensed DigiLocker Service Providers for the purpose of access

Locker, gateways and repository services using web or mobile based Digital Locker Portal.

(3) Digital Locker Portal shall provide access to repositories and access gateway for issuers to issue and requesters to access digitally signed or equivalently authenticated electronic records respectively in a uniform way in real-time by making available Digital Locker Directory to the users.

(4) Digital Locker Directory shall provide following details:

(a) issuer ID (name, ID, registration date), Requester ID (name, URL, date of empanelment, contact details), Gateway ID (name, URL, date of empanelment, contact details) and empanelled repositories (name, URL, date of empanelment, contact details);

(b) repository and gateway empanelment guidelines, standards, application form, and other particulars;

(c) electronic workflow to request, approve, and publish new ID for new issuers, gateways & repositories, as the case may be; and

(d) any other information as prescribed by the Controller of Digital Locker.

5. DigiLocker Standards:

Standards for DigiLocker eco system will be notified by the Department of Electronics & Information Technology (DeitY), Government of India.

6. Appointment of Controller and other officers:

1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Digital Locker for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers, other officers and employees as it deems fit.

2) The Controller shall discharge his functions under this Act subject to the general control and directions of DeitY.

3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers other officers and employees shall be such as may be prescribed by the Central Government.

5) The Head Office and Branch Office of the Office of the Controller shall be at such places as DeitY may specify, and these may be established at such places as DeitY may think fit.

6) There shall be a seal of the Office of the Controller.

7. The Controller may perform all or any of the following functions, namely:

1) Grant licenses to DigiLocker service providers;

2) exercising supervision over the activities of the DigiLocker Service Providers;

3) specifying the conditions subject to which the DigiLocker Service Providers shall conduct their business;

4) specify the conditions under which documents from issuers are made available to DigiLocker service providers.

5) specify the conditions under which documents accessed by requesters are made available to DigiLocker service providers

6) specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of DigiLocker Services;

7) specifying the form and manner in which accounts shall be maintained by the DigiLocker service provider;

8) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

9) facilitating the establishment of any electronic system by a Service Provider either solely or jointly with other Service Providers and regulation of such systems;

10) specifying the manner in which the Service Providers shall conduct their dealings with the subscribers;

11) resolving any conflict of interests between the Service Providers and the subscribers;

12) laying down the duties of the Service Providers;

13) maintaining a data-base containing the disclosure record of every DigiLocker Service Providers containing such particulars as may be specified by regulations, which shall be accessible to public.

8. Licensing of DigiLocker Service Providers:

(1) The following may apply for grant of a licence to become a DigiLocker Service Provider, namely:-

(a) an individual , being a citizen of India and having a capital of five crores of rupees or more in his business or profession.

(b) a company havingï

i. paid up capital of not less than five crores of rupees; and

ii. net worth of not less than fifty crores of rupees: Provided that no company in which the equity share capital held in aggregate by the Non-resident Indians, Foreign Institutional Investors, or foreign companies, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence: Provided further that in a case where the company has been

registered under the Companies Act, 1956 (1 of 1956) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as DigiLocker Service Provider, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of its majority shareholders holding at least 51% of paid equity capital, being the Hindu Undivided Family, firm or company: Provided also that the majority shareholders referred to in the second proviso shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company: Provided also that the majority shareholders of a company referred to in the second proviso whose net worth has been determined on the basis of such majority shareholders, shall not sell or transfer its equity shares held in such company- (i) unless such a company acquires or has its own net worth of not less than fifty crores of rupees; (ii) without prior approval of the Controller of Digital Locker;

(c) a firm having ï

i. capital subscribed by all partners of not less than five crores of rupees; and

ii. net worth of not less than fifty crores of rupees: Provided that no firm, in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence: Provided further that in a case where the firm has been registered under the Indian Partnership Act, 1932 (9 of 1932) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as DigiLocker service provider, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of all of its partners: Provided also that the partners referred to in the second proviso shall not include Non-resident Indian and foreign national: Provided also that the partners of a firm referred to in the second proviso whose net worth has been determined on the basis of such partners, shall not sell or transfer its capital held in such firm- (i) unless such firm has acquired or has its own

net worth of not less than fifty crores of rupees; (ii) without prior approval of the Controller;

(d) Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.

Explanation.- For the purpose of this rule,-

i. "company" shall have the meaning assigned to it in clause 17 of section 2 of the Income-tax Act, 1961 (43 of 1961);

ii. "firm", "partner" and "partnership" shall have the meanings respectively assigned to them in the Indian Partnership Act, 1932 (9 of 1932); but the expression "partner" shall also include any person who, being a minor has been admitted to the benefits of partnership;

iii. "foreign company" shall have the meaning assigned to it in clause (23A) of section 2 of the Income-tax Act, 1961 (43 of 1961);

iv. "net worth" shall have the meaning assigned to it in clause (ga) of subsection (1) of section 3 of the Sick Industrial Companies (Special Provisions) Act, 1985 (1 of 1986);

v. "Non-resident" shall have the meaning assigned to it as in clause 26 of section 2 of the Income-tax Act, 1961 (43 of 1961).

(2) The applicant being an individual, or a company, or a firm under sub-rule (1), shall submit a performance bond or furnish a banker's guarantee from a scheduled bank in favour of the Controller in such form and in such manner as may be approved by the Controller for an amount of not less than five crores of rupees and the performance bond or banker's guarantee shall remain valid for a period of six years from the date of its submission: Provided that the company and firm referred to in the second proviso to clause (b) and the second proviso to clause (c) of sub-rule (1) shall submit a performance bond or furnish a banker's guarantee for ten crores of rupees: Provided further that nothing in the first proviso shall apply to the company or firm after it has acquired or has its net worth of fifty crores of rupees.

(3) Without prejudice to any penalty which may be imposed or prosecution may be initiated for any offence under the Act or any other law for the time being in force, the performance bond or banker's guarantee may be invokedï

a) when the Controller has suspended the licence under sub-section (2) of section 25 of the Act; or

b) for payment of an offer of compensation made by the Controller; or

c) for payment of liabilities and rectification costs attributed to the negligence of the DigiLocker service provider, its officers or employees; or

d) for payment of the costs incurred in the discontinuation or transfer of operations of the licensed DigiLocker service provider, if the DigiLocker service provider's licence or operations is discontinued; or

e) any other default made by the DigiLocker service provider in complying with the provisions of the Act or rules made thereunder. Explanation.- "transfer of operation" shall have the meaning assigned to it in clause (47) of section 2 of the Income-tax Act, 1961 (43 of 1961).

9. **Location of the Facilities:**

The infrastructure associated with all functions of DigiLocker system as well as maintenance of Directories containing information about the status of DigiLocker system shall be installed at any location in India.

10. **Submission of Application:**

(1) Every application for a licensed DigiLocker service provider shall be made to the Controller,-

a) in the form given at Schedule-I; and

b) in such manner as the Controller may, from time to time, determine, supported by such documents and information as the Controller may require and it shall inter alia include-

i. a DigiLocker Practice Statement (DPS);

ii. a statement including the procedures with respect to identification of the applicant;

iii. a statement for the purpose and scope of DigiLocker technology, management, or operations to be outsourced;

iv. certified copies of the business registration documents of DigiLocker service provider that intends to be licensed;

v. a description of any event, particularly current or past insolvency, that could materially affect the applicant's ability to act as a DigiLocker service provider;

vi. an undertaking by the applicant that to its best knowledge and belief it can and will comply with the requirements of its DigiLocker Practice Statement;

vii. an undertaking that the DigiLocker service provider's operation would not commence until its operation and facilities associated with the functions of generation, issue and management of DigiLocker system are audited by the auditors and approved by the Controller in accordance with rule 31;

viii. an undertaking to submit a performance bond or banker's guarantee in accordance with sub-rule (2) of rule 8 within one month of Controller indicating his approval for the grant of licence to operate as a DigiLocker service provider;

c) any other information required by the Controller.

(2) Every application for issue of a license shall be accompanied by-

a) a DigiLocker practice statement;

b) a statement including the procedures with respect to identification of the applicant;

c) payment of such fees, not exceeding one lac rupees as may be prescribed by the Central Government;

d) such other documents, as may be prescribed by the Central Government.

11. Procedure for grant or rejection of license :

The Controller may, on receipt of an application under sub-section (1) of section 4, after considering the documents accompanying the application and such other factors, as he deems fit, grant the license or reject the application: Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

12. **Fee:**

(1) The application for the grant of a licence shall be accompanied by a non-refundable fee of one lac rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(2) The application submitted to the Controller for renewal of DigiLocker service provider's licence shall be accompanied by a non-refundable fee of twenty five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(3) Fee or any part thereof shall not be refunded if the licence is suspended or revoked during its validity period.

13. **Cross Certification**:

The licensed DigiLocker service provider shall have arrangement for cross certification with other licensed DigiLocker service providers within India which shall be submitted to the Controller before the commencement of their

operations as per rule 30: Provided that any dispute arising as a result of any such arrangement between the DigiLocker service providers; or between DigiLocker service providers or DigiLocker service provider and the Subscriber, shall be referred to the Controller for arbitration or resolution.

14. **Validity of licence:**

(1) A licence shall be valid for a period of ten years from the date of its issue.

(2) The licence shall not be transferable or heritable.

15. **Suspension of Licence:**

(1) The Controller may by order suspend the licence in accordance with the provisions contained in subrule (3).

(2) The licence granted to the persons referred to in clauses (a) to (c) of subrule (1) of rule 8 shall stand suspended when the performance bond submitted or the banker's guarantee furnished by such persons is invoked under sub-rule (2) of that rule.

(3) The Controller may, if he/she is satisfied after making such inquiry, as he/she may think fit, that a DigiLocker service Provider has ï

(a) made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the license was granted;

(c) failed to maintain the standards specified in rule (5);

(d) contravened any provisions of this Act, rule, regulation or order made there under, revoke the license: Provided that no license shall be revoked unless the DigiLocker service provider has been given a

reasonable opportunity of showing cause against the proposed revocation.

(4) The Controller may, if he/she has reasonable cause to believe that there is any ground for revoking a license under subrule (3) by order suspend such license pending the completion of any enquiry ordered by him/her: Provided that no license shall be suspended for a period exceeding ten days unless the DigiLocker service provider has been given a reasonable opportunity of showing cause against the proposed suspension.

(5) No DigiLocker service provider whose license has been suspended shall provide any access or sharing of documents and shall as per procedure, make provisions for transfer of repository / documents to another service provider/Receiver as specified by the Controller.

16. **Renewal of licence:**

(1) The provisions of rule 8 to rule 14, shall apply in the case of an application for renewal of a licence as it applies to a fresh application for licensed DigiLocker service provider.

(2) A DigiLocker service provider shall submit an application for the renewal of its licence not less than ninety days before the date of expiry of the period of validity of licence.

(3) The application for renewal of licence may be submitted in the form of electronic record subject to such requirements as the Controller may deem fit.

(4) An application for renewal of a license shall be ï

a) in such form;

b) accompanied by such fees, not exceeding twenty five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the license:

17**. Issuance of Licence:**

(1) The Controller may, within four weeks from the date of receipt of the application, after considering the documents accompanying the application and such other factors, as he/she may deem fit, grant or renew the licence or reject the application: Provided that in exceptional circumstances and for reasons to be recorded in writing, the period of four weeks may be extended to such period, not exceeding eight weeks in all as the Controller may deem fit.

(2) If the application for licensed DigiLocker service provider is approved, the applicant shall-

(a) submit a performance bond or furnish a banker's guarantee within one month from the date of such approval to the Controller in accordance with sub-rule (2) of rule 8; and

(b) execute an agreement with the Controller binding him/her self to comply with the terms and conditions of the licence and the provisions of the Act and the rules made thereunder.

18. **Refusal of Licence:**

(1)The Controller may refuse to grant or renew a licence if-

a) the applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or

b) the applicant is in the course of being wound up or liquidated; or

c) a receiver has, or a receiver and manager have, been appointed by the court in respect of the applicant; or

d) the applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these rules; or the Controller has invoked performance bond or banker's guarantee; or

e) a DigiLocker service provider commits breach of, or fails to observe and comply with, the procedures and practices as per the DigiLocker Practice Statement; or

f) a DigiLocker service provider fails to conduct, or does not submit, the returns of the audit in accordance with rule 41; or

g) the audit report recommends that the DigiLocker service provider is not worthy of continuing DigiLocker service provider's operation; or

h) a DigiLocker service provider fails to comply with the directions of the Controller.

19. Representations upon opening of DigiLocker account A DigiLocker service provider while opening a DigiLocker account shall certify that ï

(a) it has complied with the provisions of this Act and the rules and regulations made there under;

20. **Notice of suspension or revocation of license:**

(1) Where the license of the DigiLocker service provider is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data-base maintained by him/her.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories. Provided that the data-base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock Provided further that the Controller may, if he/she considers necessary, publicize the contents of the data-base in such electronic or other media, as he/she may consider appropriate.

21. Power to delegate:

The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

22. Power to investigate contraventions:

(1) The Controller or any officer authorized by him/her in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made there under.

(2) The Controller or any officer authorized by him/her in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

23. Access to computers and data:

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorized by him/her shall, if he/she has reasonable cause to suspect that any contravention of the provisions of this chapter made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorized by him/her may, by order, direct any person in charge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him/her with such reasonable technical and other assistant as he/she may consider necessary.

24. DigiLocker service providers to follow certain procedures:

Every DigiLocker service provider shall-

a) ensure that the document URI and other data provided by issuers and requesters is stored and/or transferred in its original state without any tampering.

b) make use of hardware, software, and procedures that are secure from intrusion and misuse:

c) provide a reasonable level of reliability in its services which arc reasonably suited to the performance of intended functions;

d) adhere to security procedures to ensure that the secrecy and privacy of the documents are assured.

e) publish information regarding its practices and current status of such procedures; and

f) observe such other standards as may be specified by regulations.

25. DigiLocker service provider to ensure compliance of the Act, etc:

Every DigiLocker service provider shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made there under.

26. Display of license:

Every DigiLocker service provider shall display its license at a conspicuous place of the premises in which it carries on its business.

27. Surrender of license:

(1) Every DigiLocker service provider whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the Controller.

(2) Where any DigiLocker service provider fails to surrender a license under sub-section (1), the person in whose favour a license is issued, shall be guilty of an offense and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

28 Disclosure:

(1) Every DigiLocker service provider shall disclose in the manner specified by regulations

(a) its DigiLocker Certificate

(b) any DigiLocker practice statement relevant thereto;

(c) notice of revocation or suspension of its DigiLocker certificate, if any; and

(2) Where in the opinion of the DigiLocker service provider any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which access to a document was granted, then, the DigiLocker service provider shall-

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

29. Governing Laws:

The DigiLocker Practice Statement of the DigiLocker service provider shall comply with, and be governed by, the laws of the country.

30. Security Guidelines for DigiLocker service provider:

(1) The DigiLocker service provider shall have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labeling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.

(2) Information Technology Security Guidelines and Security Guidelines for DigiLocker service provider aimed at protecting the integrity, confidentiality and availability of service of DigiLocker service provider are given in Schedule-II and Schedule-III respectively.

(3) The DigiLocker service provider shall formulate its Information Technology and Security Policy for operation complying with these guidelines and submit it to the Controller before commencement of operation: Provided that any change made by the DigiLocker service provider in the Information Technology and Security Policy shall be submitted by it within two weeks to the Controller.

31. Commencement of Operation by Licensed DigiLocker service provider:

(1) The licensed DigiLocker service provider shall commence its commercial operation only after

(a) it has confirmed to the Controller the adoption of DigiLocker Practice Statement;

(b) the installed facilities and infrastructure associated with all functions of management of DigiLocker system have been audited by the accredited auditor in accordance with the provisions of rule 41; and

(c) it has submitted the arrangement for cross certification with other licensed DigiLocker service provider within India to the Controller.

32. Requirements Prior to Cessation as DigiLocker service provider:

(1) Before ceasing to act as a DigiLocker service provider, a DigiLocker service provider shall,

a) give notice to the Controller of its intention to cease acting as a DigiLocker service provider: Provided that the notice shall be made one hundred eighty days before ceasing to act as a DigiLocker service provider or ninety days before the date of expiry of licence;

b) will follow the data retention and data migration guidelines notified by DeitY.

c) advertise one hundred twenty days before the expiry of licence or ceasing to act as DigiLocker service provider, as the case may be, the intention in such daily newspaper or newspapers and in such manner as the Controller may determine;

d) notify its intention to cease acting as a DigiLocker service provider to the subscriber, issuers and requesters of each documents available in its system:

e) the notice shall be sent to the Controller, affected subscribers, issuers and requesters by digitally signed e-mail and registered post;

f) make a reasonable effort to ensure that discontinuing its DigiLocker services causes minimal disruption to its subscribers;

g) make reasonable arrangements for preserving the records for a period of seven years;

h) pay reasonable restitution (not exceeding the cost involved in opening a DigiLocker account) to subscribers for ceasing DigiLocker services;.

33. Database of DigiLocker Service Providers:

(1) The Controller shall maintain a database of the disclosure record of every DigiLocker service provider, containing inter alia the following details:

a) the name of the person/names of the Directors, nature of business, Income tax Permanent Account Number, web address, if any, office and residential

address, location of facilities associated with functions of DigiLocker system, voice and facsimile telephone numbers, electronic mail address(es), administrative contacts and authorized representatives;

b) current and past versions of DigiLocker Practice Statement of DigiLocker service provider;

c) time stamps indicating the date and time of-

i. grant of licence;

ii. confirmation of adoption of DigiLocker Practice Statement and its earlier versions by DigiLocker service provider;

iii. commencement of commercial operations of DigiLocker system by the DigiLocker service provider;

iv. revocation or suspension of licence of DigiLocker service provider;

34. The manner in which Digital Locker System be used by Subscriber:

(1) A Digital Locker shall be used by the subscriber in the following manner:

(a) accesses and registers for Digital Locker on the web or mobile based Digital Locker Portal;

(b) uploads document, digitally signs the documents in the digital locker as provided by the DigiLocker Service Provider;

(c) accesses documents from issuers using the document URIs available in the DigiLocker account.

(d) grants access to the requester to access appropriate Government issued records by providing unique document URI;

(e) provides access to the issuer to deposit document URIs; and

(f) as prescribed by the Controller of Digital Locker from time to time.

35. The manner in which Digital Locker System be used by Requester:

(1) A Digital Locker shall be used by the requester in the following manner:

(a) registers itself with the Controller of Digital Locker specified web portal;

(b) accesses subscriberôs appropriate issued documents based on the URI; and

(c) uses licensed gateway providers to access documents stored across certified repositories;

(d) as prescribed by the Controller of Digital Locker from time to time.

36. The manner in which Digital Locker System be used by Issuer:

(1) A Digital Locker shall be used by the issuer in the following manner:

(a) registers itself with the Controller of Digital Locker specified web portal;

(b) issues new digital records in the format as prescribed by the Controller of Digital Locker and also provides older digitized records to the subscriber, which are verifiable, shareable, accessible and printable;

(c) chooses repository to preserve and retain issued records;

(d) uses the integration interfaces, to:

(i) Push URI to Digital Locker: to push the URIôs of all the records available in their repositories so that the same can be displayed to the subscriber, so as to notify the subscriber that the issuer has following documents linked to the subscriberôs account.

(ii) Pull URI Request API: to allow the subscriber to query the issuer repository by providing subscriberôs identifier applicable to issuer organization to enable issuer to provide the URIôs of all the records that are linked to the identifiers submitted by the subscriber.

(e) as prescribed by the Controller of Digital Locker from time to time.

37. Role of DigiLocker Service Providers:

(1) The Digital Locker System shall be supported by following DigiLocker service providers:

a) Digital Locker portals,

b) repositories

c) access gateways

(2) Controller of Digital Locker to grant licenses to service providers to set up Digital Locker portals, access gateways and repositories for efficient use of Digital Locker System for the benefit of subscribers, issuers and requesters.

(3) Every licensed service provider to conform to the binding licensing terms, including the standards, guidelines and specifications as laid down by the Controller of Digital Locker.

38. Appointment of Grievance Officer by the DigiLocker Service Provider for dispute resolution:

(1) Every DigiLocker Service Provider shall publish on its website the name of Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of :

(i) access or usage of Digital Locker or Digital Locker System by any unauthorised person; or

(ii) violation of licensing terms,

may notify their complaints against such access or usage or violation of licensing terms to such Grievance Officer.

(2) The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

(3) An aggrieved party may appeal to the Controller of Digital Locker against the order of the Grievance Officer within 15 days from the date of receipt of such order.

39. Suspension of Digital Locker account.

(1) Subject to the provisions of sub-section

(2), the DigiLocker service provider which has provided a DigiLocker account may suspend such DigiLocker account ï

(a) on receipt of a request to that effect from ï

(i) the subscriber listed in the DigiLocker account; or

(ii) any person duly authorized to act on behalf of that subscriber;

(b) if it is of opinion that the DigiLocker account should be suspended in public interest

(2) A DigiLocker account shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a DigiLocker account under this section, the DigiLocker service provider shall communicate the same to the subscriber.

40. Control of DigiLocker account credentials:

(1) Every subscriber shall exercise reasonable care to retain control of the DigiLocker account credentials and take all steps to prevent its disclosure

(2) If the DigiLocker account credentials have been compromised, then, the subscriber shall communicate the same without any delay to the DigiLocker service provider in such manner as may be specified by the regulations.
Explanation - For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the DigiLocker service provider that the DigiLocker account credentials have been compromised.

41. Fees for opening DigiLocker account:

(1) The DigiLocker service provider shall charge such fee not exceeding five thousand rupees as may be prescribed by the Central Government, to be paid to the DigiLocker service provider

(2) Where fees are payable, DigiLocker service provider shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing fee schedule on a nominated website.

(3) No fee is to be levied for access to DigiLocker Practice Statement via Internet. A fee may be charged by the DigiLocker service provider for providing printed copies of its DigiLocker Practice Statement.

42. Audit:

(1) The DigiLocker service provider shall get its operations audited annually by an auditor and such audit shall include inter alia,-

a) security policy and planning;

b) physical security;

c) technology evaluation;

d) DigiLocker service provider's services administration;

e) relevant DigiLocker Practice Statement;

f) compliance to relevant DigiLocker Practice Statement;

g) contracts/agreements;

h) regulations prescribed by the Controller;

i) policy requirements of DigiLocker Rules,.

(2) The DigiLocker service provider shall conduct,-

a) half yearly audit of the Security Policy, physical security and planning of its operation;

b) a quarterly audit of its system and all associated interfaces, systems, tools and processes.

(3) The DigiLocker service provider shall submit copy of each audit report to the Controller within four weeks of the completion of such audit and where irregularities are found, the DigiLocker service provider shall take immediate appropriate action to remove such irregularities.

43. Auditor's relationship with DigiLocker service provider:

(1) The auditor shall be independent of the DigiLocker service provider being audited and shall not be a software or hardware vendor which is, or has been providing services or supplying equipment to the said DigiLocker service provider.

(2) The auditor and the DigiLocker service provider shall not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

44. Confidential Information

(1) The following information shall be confidential namely:-

a) DigiLocker account application, whether approved or rejected;

b) DigiLocker account information collected from the subscriber or elsewhere as part of the registration;

c) subscriber agreement.

45. Access to Confidential Information:

(1) Access to confidential information by DigiLocker service provider 's operational staff shall be on a "need-to-know" and "need-to-use" basis. The process of maintaining confidentiality of information should be included in the DigiLocker practise statement.

(2) Paper based records, documentation and backup data containing all confidential information as prescribed in rule 33 shall be kept in secure and locked container or filing system, separately from all other records. The back up of all information should also be kept offsite in the Disaster recovery facility.

(3) The confidential information shall not be taken out of the country except in a case where a properly constitutional warrant or other legally enforceable document is produced to the Controller and he/she permits to do so.

46. Protection of action taken in good faith:

No suit, prosecution or other legal proceeding shall lie against the Government, the Controller of Digital Locker, and officers and staff of Controller of Digital Locker Secretariat for anything which is in good faith done or intended to be done in pursuance of these rules.

Schedule - I

Form for Application for grant of Licence to be a DigiLocker Service Provider

For Individual

1. Full Name * ---------- Last Name/Surname ---------- First Name _____ Middle Name _____

2. Have you ever been known by any other name? If Yes, Last Name/Surname _____First Name _____ Middle Name _____

3. Address

A. Residential Address * Flat/Door/Block No. _____ Name of Premises/Building/Village _____
Road/Street/Lane/Post Office _____
Area/Locality/Taluka/Sub-Division _____
Town/City/District _____State/Union Territory _____ Pin : _____ Telephone No. _____
Fax _____ Mobile Phone No. _____

B. Office Address * Name of Office _____
Flat/Door/Block No. _____ Name of Premises/Building/Village _____
Road/Street/Lane/Post Office _____
Area/Locality/Taluka/Sub-Division _____
Town/City/District _____ State/Union Territory _____ Pin : _____ Telephone No. _____ Fax _____

4. Address for Communication * Tick ✓ as applicable A or B

5. Father's Name * _____ Last Name/Surname _____First Name _____ Middle Name _____

6. Sex * (For Individual Applicant only) Tick ✓ as applicable : Male/ Female

7. Date of Birth (dd/mm/yyyy) * ____/____/_____

8. Nationality * _____

9. Credit Card Details/Credit Card Type _____ Credit Card No. _____ Issued By _____

10. E-mail Address _____

11. Web URL address _____

12. Passport Details # Passport No. _____ Passport issuing authority _____ Passport expiry date (dd/mm/yyyy) ____/____/____

13. Voter's Identity Card No. # _____

14. Income Tax PAN No. # _____

15. ISP Details ISP Name * _____ ISP's Website Address, if any _____ Your User Name at ISP, if any _____

16. Personal Web page URL address, if any _____

17. Capital in the business or profession * Rs._____ (Attach documentary proof)

For Company/Firm/Body of Individuals/Association of Persons/Local Authority

18. Registration Number * _____

19. Date of Incorporation/Agreement/Partnership * ____/____/_____

20. Particulars of Business, if any: * Head Office _____ Name of Office _____ Flat/Door/Block No. _____ Name of Premises/Building/Village _____ Road/Street/Lane/Post Office _____ Area/Locality/Taluka/Sub-Division _____ Town/City/District _____ Pin _____ State/Union Territory _____ Telephone No. _____ Fax _____

_____ Web page URL address, if any _____ No. of Branches _____ Nature of Business _____ _____

21. Income Tax PAN No. * _____

22. Turnover in the last financial year Rs._____

23. Net worth * Rs._____ (Attach documentary proof)

24. Paid up Capital * Rs._____ (Attach documentary proof)

25. Insurance Details Insurance Policy No. * _____ Insurer Company * _____

26. Names, Addresses etc. of Partners/Members/Directors (For Information about more persons, please add separate sheet(s) in the format given in the next page) * No. of Partners/Members/Directors _____ Details of Partners/Members/Directors

A. Full Name Last Name/Surname _____ First Name _____ Middle Name _____

B. Address Flat/Door/Block No. _____ Name of Premises/Building/Village _____ Road/Street/Lane/Post Office _____ Area/Locality/Taluka/Sub-Division _____ Town/City/District _____ State/Union Territory Pin _____

Telephone No. _____ Fax No. _____ Mobile Phone No. _____

C. Nationality _____ In case of foreign national, Visa details_____

D. Passport Details # Passport No. _____ Passport issuing authority _____Passport expiry date _____

E. Voter's Identity Card No. # _____

F. Income Tax Pan No. # _____

G. E-mail Address _____

H. Personal Web page URL, if any _____

27. Authorised Representative * Name _____ Flat/Door/Block No. _____ Name of Premises/Building/Village _____ Road/Street/Lane/Post Office _____ Area/Locality/Taluka/Sub-Division _____ Town/City/District _____ Pin _____ State/Union Territory _____ Telephone No. _____ Fax _____ Nature of Business _____

For Government Ministry/Department/Agency/Authority

28. Particulars of Organisation: * Name of Organisation _____ Administrative Ministry/Department _____ Under State/Central Government _____ Flat/Door/Block No. _____ Name of Premises/Building/Village _____ Road/Street/Lane/Post Office _____ a/Locality/Taluka/Sub-Division _____ Town/City/District _____ Pin _____ State/Union Territory _____ Telephone No. _____ Fax No. _____ Web page URL Address _____ Name of the Head of Organisation _____ Designation _____ E-mail Address _____

29. Bank Details Bank Name * _____ Branch * _____ Bank Account No. * _____ Type of Bank Account * _____

30. Whether bank draft/pay order for licence fee enclosed * : Y / N If Yes

Name of Bank _____ Draft/pay order No. _____ Date of Issue _____ Amount _____

31. Location of facility in India for providing of Digital Locker services * _____

32. Whether undertaking for Bank Guarantee/Performance Bond attached * : Y / N (Not applicable if the applicant is a Government Ministry/Department/Agency/ Authority)

33. Whether DigiLocker Practice Statement is enclosed * : Y / N

34. Whether certified copies of business registration document are enclosed : Y / N (For Company/Firm/Body of Individuals/Association of Persons/Local Authority) If yes, the documents attached: ii) ..... iii) ..... iv) .....

35. Any other information _____ _____

Date

Signature of the Applicant

Instructions : 1. Columns marked with * are mandatory.

2. For the columns marked with #, details for at least one is mandatory.

3. Column No. 1 to 17 are to be filled up by individual applicant.

4. Column No. 18 to 27 are to be filled up if applicant is a Company/Firm/Body of Individuals/Association of Persons/Local Authority.

5. Column No. 28 is to be filled up if applicant is a Government organisation.

<End of Document>

Schedule II

[See rule 29(2)]

Information Technology (IT) Security Guidelines

1. Introduction: This document provides guidelines for the implementation and management of Information Technology Security. Due to the inherent dynamism of the security requirements, this document does not provide an exact template for the organizations to follow. However, appropriate suitable samples of security process are provided for guidelines. It is the responsibility of the organizations to develop internal processes that meet the guidelines set forth in this document. The following words used in the Information Technology Security Guidelines shall be interpreted as follows:

- shall: The guideline defined is a mandatory requirement, and therefore must be complied with.
- should: The guideline defined is a recommended requirement. Noncompliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented.
- must: The guideline defined is a mandatory requirement, and therefore must be complied with.
- may: The guideline defined is an optional requirement. The implementation of this guideline is determined by the organisation's requirement.

2. Implementation of an Information Security Programme: Successful implementation of a meaningful Information Security Programme rests with the support of the top management. Until and unless the senior managers of the organization understand and concur with the objectives of the information security programme its ultimate success is in question. The Information Security Programme should be broken down into specific stages as follows:

(a) Adoption of a security policy;

(b) Security risk analysis;

(c) Development and implementation of an information classification system;

(d) Development and implementation of the security standards manual;

(e) Implementation of the management security self-assessment process;

(f) On-going security programme maintenance and enforcement; and

(g) Training.

The principal task of the security implementation is to define the responsibilities of persons within the organization. The implementation must be based on the general principle that the person who is generating the information is also responsible for its security. However, in order to enable him/her to carry out his/her responsibilities in this regard, proper tools, and environment need to be established. When different pieces of information at one level are integrated to form higher value information, the responsibility for its security needs also must go up in the hierarchy to the integrator and should require higher level of authority for its access. It must be absolutely clear with respect to each information as to who is its owner, its custodian, and its users. It is the duty of the owner to assign the right classification to the information so that the required level of security can be enforced. The custodian of information is responsible for the proper implementation of security guidelines and making the information available to the users on a need to know basis.

3. Information Classification: Information assets must be classified according to their sensitivity and their importance to the organization. Since it is unrealistic to expect managers and employees to maintain absolute control over all information within the boundaries of the organization, it is necessary to advise them on which types of information are considered more sensitive, and how the organization would like the sensitive information handled and protected. Classification, declassification, labeling, storage, access, destruction and reproduction of classified data and the administrative overhead this process will create must be considered. Failure to maintain a balance between the value of the information classified and the administrative burden the classification system places on the organization will result in long-term difficulties in achieving success.

Confidential is that classification of information of which unauthorized disclosure/ use could cause serious damage to the organization, e.g. strategic planning documents.

Restricted is that classification of information of which unauthorized disclosure/ use would not be in the best interest of the organization and/or its customers, e.g. design details, computer software (programs, utilities), documentation, organization personnel data, budget information.

Internal use is that classification of information that does not require any degree of protection against disclosure within the company, e.g. operating procedures, policies and standards inter office memorandums.

Unclassified is that classification of information that requires no protection against disclosure e.g. published annual reports, periodicals. While the above classifications are appropriate for a general organization view point, the following classifications may be considered:

Top **Secret**: It shall be applied to information unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for Nation's closest secrets and to be used with great reserve.

Secret: This shall be applied to information unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

Confidentiality: This shall be applied to information unauthorized disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its functioning. Most information will on proper analysis be classified no higher than confidential.

Restricted: This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.

Unclassified: This is the classification of information that requires no protection against disclosure.

4. Physical and Operational Security :

4.1 Site Design (1) The site shall not be in locations that are prone to natural or man- disasters, like flood, fire, chemical contamination and explosions.

(2) As per nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.

(3) Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies. Further, the construction must be tamper-evident.

(4) Materials used for the construction of the operational site shall be fire resistant and free of toxic chemicals.

(5) External walls shall be constructed of brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows shall be fortified with study mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.

(6) Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.

(7) Automatic fire detection, fire suppression systems and equipment in compliance with requirement specified by the Fire Brigade or any other agencies of the Central or State Government shall be installed at the operational site.

(8) Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.

(9) Any facility that supports mission-critical and sensitive applications must be located and designed for repairability, relocation and reconfiguration. The ability to

relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/disaster recovery plan.

4.2 Fire Protection (1) Combustible materials shall not be stored within hundred meters of the operational site.

(2) Automatic fire detection, fire suppression systems and audible alarms as prescribed by the Fire Brigade or any other agency of the Central or State Government shall be installed at the operational site.

(3) Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.

(4) Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems shall be carried out.

(5) Procedures for the safe evacuation of personnel in an emergency shall be visibly pasted/displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.

(6) There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

4.3 Environmental Protection (1) Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms.

(2) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

(3) Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.

(4) Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

4.4 Physical Access (1) Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for

operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.

(2) Biometric physical access security systems shall be installed to control and audit access to the operational site.

(3) Physical access to the operational site at all times shall be controlled and restricted to authorised personnel only. Personnel authorized for limited physical access shall not be allowed to gain unauthorized access to restricted area within operational site.

(4) Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years.

(5) Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorised access.

(6) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.

(7) Emergency exits shall be tested periodically to ensure that the access security systems are operational.

(8) All opening of the Data Centre should be monitored round the clock by surveillance video cameras.

5. Information Management

5.1 System Administration (1) Each organization shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending upon the complexity and security needs of a system or application, the System Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information.

(2) Organisations shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.

(3) The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Administrator.

(4) Any password used for the system administration and operation of trusted services must not be written down (in paper or electronic form) or shared with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organization. Every instance of usage of administrator's passwords must be documented.

(5) Periodic review of the access rights of all users must be performed.

(6) The System Administrator must promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access. Reactivation of the user's account must be authorized in writing by the System Administrator (Digitally signed e-mail may be acceptable).

(7) The System Administrator must take steps to safeguards classified information as prescribed by its owner.

(8) The System Administrator must authorize privileged access to users only on a need-to-know and need-to-do basis and also only after the authorization is documented.

(9) Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.

(10) All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.

(11) The System Administrator together with the system support staff, shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information.

(12) The System Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.

(13) The System Administrator should ensure that no generic user is enabled or active on the system.

5.2 Sensitive Information Control (1) Information assets shall be classified and protected according to their sensitivity and criticality to the organization.

(2) Procedures in accordance with para 8.3 of these Guidelines must be in place to handle the storage media, which has sensitive and classified information.

(3) All sensitive information stored in any media shall bear or be assigned an appropriate security classification.

(4) All sensitive material shall be stamped or labeled accordingly.

(5) Storage media (i.e. external hard disks, usb storage devices, CD/DVDôs, tapes etc.) containing sensitive information shall be secured according to their classification.

(6) Electronic communication systems, such as router, switches, network device and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard should be documented.

(7) Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged or affected media both internal (e.g. hard disk/SAN storage) and external (e.g. external hard disks, usb storage devices, CD/DVDôs, tapes etc.) to the system. Preferably such affected/corrupted/damaged media both internal and external to the system shall be destroyed.

5.3 Sensitive Information Security (1) Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorized persons.

(2) Highly sensitive information shall be classified in accordance with para 3.

(3) Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (e.g., password). Security packages must be installed which partition or provide authorization to segregated directories/files.

(4) Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.

(5) Removable electronic storage media containing sensitive information and data must be clearly labeled and secured.

(6) Hard disks containing sensitive information and data must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

5.4 Third Party Access (1) Access to the computer systems by other organisations shall be subjected to a similar level of security protection and controls as in these Information Technology security guidelines.

(2) In case the Data Centre uses the facilities of external service/facility provider (outsourcer) for any of their operations, the use of external service/facility providers (e.g. outsourcer) shall be evaluated in light of the possible security exposures and risks involved and all such agreements shall be approved by the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/operational site.

(3) The external service/facility provider (e.g. outsourcer) shall provide an equivalent level of security controls as required by these Information Technology Security Guidelines.

5.5 Prevention of Computer Misuse (1) Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.

(2) Each organization shall provide adequate information to all persons, including management, systems developers and programmers, end-users, and third party users warning them against misuse of computers.

(3) Effective measures to deal expeditiously with breaches of security shall be established within each organisation. Such measures shall include:

(i) Prompt reporting of suspected breach;

(ii) Proper investigation and assessment of the nature of suspected breach;

(iii) Secure evidence and preserve integrity of such material as relates to the discovery of any breach;

(iv) Remedial measures.

(4) All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.

(5) Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedures shall include:

(i) The role of the System Administrator, System Security Administrator and management;

(ii) Procedure for investigation;

(iii) Areas for security review; and

(iv) Subsequent follow-up action

6. System integrity and security measures

6.1 Use of Security Systems or Facilities (1) Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorised users from gaining entry to the information system and to prevent unauthorised access to data.

(2) Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

6.2 System Access Control (1) Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorise issuance of user identification (ID) and resource privileges. (2) Access to information system resources like memory, storage devices etc., sensitive utilities and data resources and programme files shall be controlled and restricted based on a "need-to-use" basis with proper segregation of duties.

(3) The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as "administrator" or "president" or "game" etc. to protect access to the system and data resources represent a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.

(4) Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Guidelines and procedures governing access authorisations shall be developed, documented and implemented.

(5) An Access Control System manual documenting the access granted to different level of users shall be prepared to provide guidance to the System Administrator for grant of access.

(6) Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.

(7) Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorised disclosure and modification.

(8) Stored passwords shall be protected by access controls from unauthorised disclosure and modification.

(9) Automatic time-out for terminal inactivity should be implemented.

(10) Audit trail of security-sensitive access and actions taken shall be logged.

(11) All forms of audit trail shall be appropriately protected against unauthorised modification or deletion.

(12) Where a second level access control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.

(13) Activities of all remote users shall be logged and monitored closely.

(14) The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (e.g. root in Linux, Unix, administrator in Windows Server). This means that there must be a user account configured for the trusted administrator. The system requires trusted users to change their effective username to gain access to root and to re-authenticate themselves before requesting access to privileged functions.

(15) The startup and shutdown procedure of the security software must be automated.

(16) Sensitive Operating System files, which are more prone to hackers must be protected against all known attacks using proven tools and techniques. That is to say no user will be able to modify them except with the permission of System Administrator.

6.3 Password Management (1) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords:

(i) Minimum of eight characters without leading or trailing blanks;

(ii) Shall be different from the existing password and the two previous ones;

(iii) Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days;

(iv) Shall not be shared, displayed or printed.

(2) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.

(3) Passwords which are easy-to-guess (e.g. user name, birth date, month, standard words etc.) should be avoided.

(4) Initial or reset passwords must be changed by the user upon first use.

(5) Passwords shall always be encrypted in storage to prevent unauthorized disclosure.

(6) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.4 Privileged User's Management (1) System privileges shall be granted to users only on a need-to-use basis.

(2) Login privileges for highly privileged accounts should be available only from Console and terminals situated within Console room.

(3) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator.

(4) Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.

(5) Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.

(6) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

6.5 User's Account Management (1) Procedures for user account management shall be established to control access to application systems and data. The procedures shall include the following:

(i) Users shall be authorised by the computer system and application owner to access the computer services

(ii) A written statement of access rights shall be given to all users.

(iii) All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.

(iv) Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorization procedures have been completed. This includes the acknowledgment of receipt of the accounts by the users.

(v) A formal record of all registered users of the computer services shall be maintained.

(vi) Access rights of users who have been transferred, or left the organisation shall be removed immediately.

(vii) A periodic check shall be carried out for redundant user accounts and access rights that are no longer required.

(viii) Ensure that redundant user accounts are not re-issued to another user.

(2) User accounts shall be suspended under the following conditions:

(i) when an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator.

(ii) immediately upon the termination of the services of an individual.

(iii) suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

6.6 Data and Resource Protection (1) All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.

(2) The operating system or security system of the computer system shall:

(i) Define user authority and enforce access control to data within the computer system;

(ii) Be capable of specifying, for each named individual, a list of named data objects (e.g. file, programme) or groups of named objects

(3) For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks.

(4) Access controls for any data and/or resources shall be determined as part of the systems analysis and design process.

(5) Application Programmer shall not be allowed to access the production system.

7. Sensitive Systems Protection (1) Security tokens/smart cards/bio-metric technologies such as Iris recognition, finger print verification technologies etc. shall be used to complement the usage of passwords to access the computer system.

(2) For computer system processing sensitive data, access by other organisations shall be prohibited or strictly controlled.

(3) For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

8. Data Centre Operations Security

8.1 Job Scheduling (1) Procedures shall be established to ensure that all changes to the job schedules are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.

(2) As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

8.2 System Operations Procedure (1) Procedures shall be established to ensure that only authorised and correct job stream and parameter changes are made.

(2) Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.

(3) Procedures shall be established to ensure that people other than authorised operators are prohibited from operating the computer equipment.

(4) Procedures shall be implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system.

8.3 Media Management (1) Responsibilities for media library management and protection shall be clearly defined and assigned.

(2) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals.

(3) Access to the media library (both on-site and off-site) shall be restricted to the authorized persons only. A list of personnel authorised to enter the library shall be maintained.

(4) The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in few hours.

(5) A media management system shall be in place to account for all media stored on-site and off-site.

(6) All incoming/outgoing media transfers shall be authorised by management and users.

(7) An independent physical inventory check of all media shall be conducted at least every six months.

(8) All media shall have external volume identification. Internal labels shall be fixed, where available.

(9) Procedures shall be in place to ensure that only authorised addition/removal of media from the library is allowed.

(10) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

8.4 Media Movement (1) Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.

(2) There shall be procedures to ensure the authorized and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.

(3) Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

9. Data Backup and Off-site Retention

(1) Back-up procedures shall be documented, scheduled and monitored.

(2) Up-to-date backups of all critical items shall be maintained to ensure the continued provision of the minimum essential level of service. These items include:

(i) Data files

(ii) Utilities programmes

(iii) Databases

(iv) Operating system software

(v) Applications system software

(vi) Encryption keys (vii) Pre-printed forms

(viii) Documentation (including a copy of the business continuity plans)

(3) One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.

(4) Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development and data conversion efforts.

(5) Data backup is required for all systems including personal computers, servers and distributed systems and databases on a real time basis with zero data loss.

(6) Critical system data and file server software must have full backups taken weekly.

(7) The backups must be kept in an area physically separate from the server. If critical system data on the LAN represents unique versions of the information

assets, then the information backups must be rotated on a periodic basis to an off-site storage location.

(8) Critical system data and file server software must have incremental backups taken on a real time basis ensuring zero data loss.

(9) Systems that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information.

(10) Each LAN/system should have a primary and backup operator to ensure continuity of business operations.

(11) The business recovery plan should be prepared and tested on a bi-annual basis and random quarterly drills should be undertaken ensure business continuity.

10. Audit Trails and Verification

(1) Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.

(2) Adequate audit trails shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) shall be analyzed. This information includes such information as who, what, when, where, and any special information such as:

(i) Success or failure of the event

(ii) Use of authentication keys, where applicable

(3) Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include:

(i) Significant computer system events (e.g. configuration updates, system crashes)

(ii) Security profile changes

(iii) Actions taken by computer operations, system administrators, system programmers, and/or security administrators

(4) The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

(5) The real time clock of the computer or communications device shall be set to Indian Standard Time (IST). Further there shall be a weekly procedure that checks and corrects drift in the real time clock.

(6) Computer system access records shall be kept for a minimum of three years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behaviour, shall be retained as per laws of the land.

(7) Computer records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.

11. Measures to Handle Computer Virus (1) Responsibilities and duties shall be assigned to ensure that all file servers and personal computers are equipped with up-to-date virus protection and detection software and malware detection & protection software.

(2) Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.

(3) All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No storage media like USB storage, external hard disks, DVDs, CDs etc. brought from outside shall be used on the data, file, computer server or personal computer on Intranet and Internet without proper screening and verification by virus detection software.

(4) A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that latest version of antivirus software is loaded on all data, file and personal computers.

(5) Procedures shall be established to limit the spread of viruses to other organization information assets. Such procedures inter alia shall include:

(i) Communication to other business partners and users who may be at risk from an infected resource

(ii) Eradication and recovery procedures

(iii) Incident report must be documented and communicated per established procedures.

(6) An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

12. Relocation of Hardware and Software

Whenever computers or computer peripherals are relocated (e.g. for maintenance, installation at different sites or storage), the following guidelines shall apply:

(i) All removable media will be removed from the computer system and kept at secure location.

(ii) Internal drives will be overwritten, reformatted or removed as the situation may be.

(iii) If applicable, ribbons will be removed from printers.

(iv) All paper will be removed from printers.

Logs should be kept for all devices being relocated or removed and sign by the supervisors of the operations.

13. Hardware and Software Maintenance

Whenever, the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:

(1) Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.

(2) Maintenance of an inventory and configuration chart of hardware.

(3) Identification and use of security features implemented within hardware.

(4) Authorization, documentation, and control of change made to the hardware.

(5) Identification of support facilities including power and air conditioning.

(6) Provision of an uninterruptible power supply.

(7) Maintenance of equipment and services.

(8) Organisation must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that contract for annual maintenance of hardware is always in place.

(9) Organisation must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.

(10) Maintenance personnel will sign non-disclosure agreements.

(11) The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.

(12) All maintenance personnel should be escorted within the operational site/ computer system and network installation room by the authorized personnel of the organisation.

(13) After maintenance, any exposed security parameters such as passwords, user IDs, and accounts will be changed or reset to eliminate any potential security exposures.

(14) If the computer system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system managers or users

shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

14. Purchase and Licensing of Hardware and Software

(1) Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organisation system or network, must be verified to comply with these Information Technology Security Guidelines prior to the signing of any contract, purchase or lease.

(2) Software, which is capable of bypassing or modifying the security system or operating system, integrity features, must be verified to determine that they conform to these Information Technology Security Guidelines. Where such compliance is not possible, then procedures shall be in place to ensure that the implementation and operation of that software does not compromise the security of the system.

(3) There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Indian Copyright Act and Information Technology Security Guidelines.

(4) It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.

(5) No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to install and test the software under evaluation.

(6) Illegally acquired or unauthorized software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorized software is detected by the System Administrator or Network Administrator, the same must be removed.

15. System Software

(1) All system software options and parameters shall be reviewed and approved by the management.

(2) System software shall be comprehensively tested and its security functionality validated prior to implementation.

(3) All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.

(4) Versions of system software installed on the computer system and communication devices shall be regularly updated.

(5) All changes proposed in the system software must be appropriately justified and approved by an authorised party.

(6) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.

(7) Procedures to control changes initiated by vendors shall be in accordance with para 21 pertaining to "Change Management".

(8) There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.

(9) System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment.

(10) Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

16. Documentation Security

(1) All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.

(2) All documentation and subsequent changes shall be reviewed and approved by an independent authorised party prior to issue.

(3) Access to application software documentation and sensitive system software documentation shall be restricted to authorised personnel on a "need-to-use" basis only.

(4) Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.

(5) Documentation shall be classified according to the sensitivity of its contents/ implications.

(6) Organisations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours.

17. Network Communication Security

(1) All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems should be protected from physical damage.

(2) The network configuration and inventories shall be documented and maintained.

(3) Prior authorization of the Network Administrator shall be obtained for making any changes to network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.

(4) Physical access to communications and network sites shall be controlled and restricted to authorized individuals only in accordance with para 4.4 pertaining to "Physical Access".

(5) Communication and network systems shall be controlled and restricted to authorized individuals only in accordance with para 6.2 ï System Access Control.

(6) As far as possible, transmission medium within the DigiLocker service provider 's operational site should be secured against electro magnetic transmission. In this

regard, use of Optical Fibre Cable and armoured cable may be preferred as transmission media as the case may be

(7) Network diagnostic tools, e.g., spectrum analyzer, protocol analyzer should be used on a need basis.

18. Firewalls

(1) Intelligent devices generally known as "Firewalls" shall be used to isolate organisation's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorized use.

(2) Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organization shall be physically and logically isolated from the Internet and any other external connection by a firewall.

(3) All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.

(4) All web servers for access by Internet users shall be isolated from other data and host servers.

19. Connectivity

(1) Organisation shall establish procedure for allowing connectivity of their computer network or computer system to non-organisation computer system or networks. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented.

(2) All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organisation's host system must adhere to the general system security and access control guidelines.

(3) The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organisation's network.

(4) As far as possible, no Internet access should be allowed to database server/ file server or server hosting sensitive data.

(5) The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

20. Network Administrator

(1) Each organization shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.

(2) Network Administrator shall regularly undertake the review of network and also take adequate measures to provide physical, logical and procedural safeguards for its security. Appropriate follow up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.

(3) System must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g., unauthorized access, virus infection and hacking.

(4) Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized.

(5) Only authorized and legal software shall be used on the network.

(6) Shared computer systems, network devices used for business applications shall comply with the requirement established in para 6 ï System Integrity and Security Measures.

21. Change Management

21.1 Change Control (1) Procedures for tracking and managing changes in application software, system software, hardware and data in the production system shall be established. Organisational responsibilities for the change management process shall be defined and assigned.

(2) A risk and impact analysis, classification and prioritisation process shall be established.

(3) No changes to a production system shall be implemented until such changes have been formally authorised. Authorisation procedures for change control shall be defined and documented.

(4) Owners/Users shall be notified of all changes made to production system which may affect the processing of information on the said production system.

(5) Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented

(6) Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented.

(7) Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented. Different versions of application software and system software must be kept in safe custody.

21.2 Testing Of Changes To Production System (1) All changes in computer resource proposed in the production system shall be tested and the test results shall be reviewed and accepted by all concerned parties prior to implementation.

(2) All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes:

(i) Test objectives,

(ii) A documented test plan, and

(iii) acceptance criteria.

21.3 Review Of Changes (1) Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorised or malicious codes.

(2) Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning.

(3) All emergency changes/fixes in computer resource in the production system shall be reviewed and approved.

(4) Periodic management reports on the status of the changes implemented in the computer resourced in the production system shall be submitted for management review.

22. Problem Management and Reporting

(1) Procedures for identifying, reporting and resolving problems, such as non-functioning of DigiLocker service provider's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review.

(2) A help desk shall be set up to assist users in the resolution of problems.

(3) A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resources.

23. Emergency Preparedness

(1) Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically.

(2) Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

24. Contingency Recovery Equipment and Services

(1) Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.

(2) The business continuity plan shall be developed which inter alia include the procedures for emergency ordering of the equipment and availability of the services.

(3) The need for backup hardware and other peripherals should be evaluated in accordance to business needs.

25. Security Incident Reporting and Response

(1) All security related incidents must be reported to central coordinator, appointed by the management to coordinate and handle security related incidents. This central coordinator shall be the single point of contact at the organization.

(2) All incidents reported, actions taken, follow-up actions, and other related information shall be documented.

(3) Procedures shall be defined for dealing with all security related incidents, including malicious software, break-ins from networks, software bugs which compromised the security of the system.

26. Disaster Recovery/Management

(1) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the facility, essential level of service will be provided. The disaster recovery framework should include:

(a) emergency procedures, describing the immediate action to be taken in case of a major incident

(b) fall back procedure, describing the actions to be taken to relocate essential activities or support services to a backup site

(c) restoration procedures, describing the action to be taken to return to normal operation at the original site

(2) The documentation should include:

(a) definition of a disaster;

(b) condition for activating the plan;

(c) stages of a crisis;

(d) who will make decisions in the crisis;

(e) role of individuals for each component of the plan;

(f) composition of the recovery team; and

(g) decision making process for return to normal operation.

3) Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.

(4) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster.

(5) Each component/aspect of the plan should have a person and a backup assigned to its execution.

(6) Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster.

(7) Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review.

(8) Disaster recovery plan should be updated regularly to ensure its continuing effectiveness.