CHAPTER 4

BUSINESS CONTINUITY MANAGEMENT

DISASTER RECOVERY AND BUSINESS CONTINUITY

Synopsis

To establish the system and non-IT related failures or disasters and to describe guidelines to develop, document, exercise and maintain an IT Disaster Recovery Plan.

Guidelines

1. The critical business processes and major causes of interruption in business activities should be identified.
2. Consequences of such disasters and related loss should be analyzed. Accordingly the contingency plans should maintain operations and make sure that availability of information for business with any error.
3. Any changes in the same should be updated to all the related personnel. Roles and responsibilities of such personnel should be clearly identified.
4. Periodically mock drills should be conducted and updated plans accordingly. The responsibilities of the individual/team should be clearly defined.
5. Organizational Business Continuity Plan (BCP) should be linked with the Disaster Recovery Plan.
6. Business Continuity Plan (BCP) should be maintained all sensitive areas. Such plans should be regularly updated.
7. Testing and updating of Business continuity plans should be made on regular basis to ensure that they are up to date and effective
8. DR Site should be activated within 4 hours or as decided by the Disaster Recovery Team after the declaration of its occurrence.
COMPLIANCE

Synopsis

To establish the rules to avoid breach of any criminal and civil law, statutory, regulatory and/or contractual obligations, and any security requirements.

Controls

Identification of Applicable Legislation

All relevant statutory, regulatory and contractual requirements should be defined explicitly and documented for each information system.

Intellectual Property Rights (IPR)

Organization should be strict to legal restrictions on the use of proprietary of purchased software products and other equipments should be tally with the organizations requirements.

Protection of Organizational Records

Important records of organization should be protected from unauthorized access, loss of data and destruction.

Should be implement of the rule for Prevention of Misuse of Organizational Information

Corporate, branch, Centre Security Committee should authorizes the use of information on a proper way and make sure the facilities and controls should be applied.

INFORMATION SYSTEM AUDIT CONSIDERATIONS

Synopsis

To information system audit considerations setup the rules to make the most of the success and to minimize intrusion to the system and network audit process.
Audits will be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents
- Ensure conformance to organization security policies
- Monitor user or system activity where appropriate

Guidelines

1. Security Audit should be conducted twice in a year by the internal audit department and MR should be responsible to ensure the same.
2. The internal audit department should plan the Security audit in such a way that organization’s operations are not affected due to the Security Audit. In any way the Audit department should review all the critical operational systems of the organization.
3. Report of the security audit should be circulated to the HOD.
4. Abstract of the Report which concerns to individual departments should be circulated to HOD’S of the department.
5. Immediate action should be taken by the department on the reported issues or proper reply should be sent to the management on each issues reported.

VSAT/LEASED LINE INSTALLATION POLICY

Synopsis

This policy describes the functions relating to providing VSAT Connectivity & Leased Line Connectivity to members.

Scope

This policy applies to all employees of organization & all the members availing the facilities relating to VSAT & Leased Line Connectivity.

Guidelines

1. Organization will provide electronic connectivity to it members through VSAT or Leased Line for smooth functioning during trading hours on member’s request and the same will be as
specified in the procedure.

2. After receiving a request from member, Membership Department should authorize and approve the same.

3. On Membership Department’s request via e-mail, Managed services should process and co-ordinate with the Service providers for necessary installations and activations.

4. If any member needs to terminate or transfer the connectivity (viz. transfer of connectivity mode is possible in case of VSAT only from one member to another member) a request for the same would be received by Membership Department and processed as per the Organization’s circulars and IT procedures in co-ordination with Managed services.

5. If any member needs to shift the connectivity mode from one location to another, a request for the same would be received by Membership Department and processed as per IT procedures in co-ordination with Managed services.

6. All the necessary records pertaining to the connectivity of V-sat / Leased Line Installation should be maintained by the concerned departments as mentioned in the IT procedures.

RESEARCH PRODUCTIVITY

As it is practically not possible to study all aspects of a process in its entirety thoroughly during the limited time period of an research, based on my methodology for conducting internal research, I conducted a review of the process & held discussions with the process owners & other key people in the process during the planning stage of research which helped us in identifying specific areas where control weaknesses & process gaps may exist, opportunities for process improvement & / or cost reduction / revenue enhancement.

Our subsequent test work, study of issues in detail & developing action plans are directed towards the issues identified. Consequently this report may not necessarily comment on all the function / process related matters perceived as important by the management.