INDIA INTERNATIONAL HOUSE LIMITED
A-6, SITE NO-IV, SAHIBABAD INDUSTRIAL AREA, GHAZIABAD

E Information Technology

1 The facility is using anti virus software at each computer node. These programs are to detect and prevent the unauthorized access/attempted access by hackers and a detailed report shall be provided to the management in case of occurance.

2 The anti virus software is being updates on regular basis.

3 All computers are having inbuilt fire walls to protect the IT system.

4 It is mandatory requirement for the operators of the established computer nodes to feed the login password to access the IT system

5 Company is having several computer nodes at the office and at shipping section of the company. No other employee is having access to the computer systems.

1. Facility is also making back up of the data in separate hard disks by the frequency of once in every 30 days.

2. Computer systems that create or update critical data on daily basis are backed up on daily basis.

3. On the devices of data back up, date and type of data and concerned section's name is being mentioned.

4. This also involve the duration of the data backup.

5. The data backup is being secured at a very secure place in the office of the top management.

6. Thus the user rights for computers are based on the job functions.

7. Facility has taken services of a computer professional for maintenance and updating the software and hardware established.

8. In case of any disaster related to information technology, services of the said professional shall be taken for effective and efficient resumption of vital company functions.

9. Any recovery from IT disaster shall contain the following"

a) Backup of data
b) Recovery of data
c) Testing
d) Maintenance Planning

10. The employees using the computer nodes are being advised to not violate the above mentioned points during the regular training programs being organized time to time by the HR department.
11. In case of detection of any violation of the IT policy and regulations by any employee, the employee shall be detached immediately from the related works area.
12. The systems shall be seized and shall be provided to data and network experts hired by company.
13. The investigations shall be done by data analyst along with chief security officer of the facility.
14. The disciplinary actions shall be decided by Top Management as per the proves and severity of the incident.
15. Same shall be recorded in the record of review log for IT violations and invalid file access.
16. The incident shall be recorded and investigation results and analysis with all possible corrections, corrective actions and preventive actions shall be communicated to Top Management by chief security officer.
17. The same shall be discussed in the security review meetings.

INDIA INTERNATIONAL HOUSE LIMITED
A-6, SITE NO-IV, SAHIBABAD INDUSTRIAL AREA, GHAZIABAD

Procedure for change of passwords of computer

Objective: To define the activities to be executed for change of the passwords on computer nodes.

Description:

i. This is the prime responsibility of the system administrator to notify the user for change of the passwords.
ii. The passwords shall be changed by the frequency of once in every 30 days.
iii. The user rights for computers are based on the job functions.
iv. The passwords on the computers are being kept confidential. Passwords shall never be chosen from easy options such as city name or date of birth.
v. List of passwords shall be creating by the system administrator every time of change of password.
vi. Only system administrator keeps the list of passwords at a secured location.
vii. Passwords shall be the combination of alphabets and numeric characters.
viii. All IT system violators shall be penalized by taking appropriate disciplinary actions against them.
ix. The disciplinary actions to be taken shall be decided by Top Management after reviewing the intensity of the matter.
x. Issues related to IT security and System Security shall be taken care by conduct of a meeting by the frequency of once in every 06 months. Top Management shall discuss the related issues with Chief Security Officer and System Administrator.

Responsibility:

System Administrator
Top Management

INDIA INTERNATIONAL HOUSE LIMITED
A-6, SITE NO-IV, SAHIBABAD INDUSTRIAL AREA, GHAZIABAD

Procedure for Recovery from Information Technology Disaster

Objective:
To describe the disaster recovery plan related to Information Technology.

Description:

1. The facility has secured the services of qualified information technology professional for disaster recovery and maintenance of established software and hardware.
2. In case of any disaster related to information technology, services of above said professional shall be taken.
3. Effective and efficient resumption of vital company functions shall be ensured in case of an unscheduled interruption.
4. Any disaster recovery plan shall contain the following ingredients:

a) Critical Assessment
b) Back up procedures
c) Recovery Procedures
d) Implementation Procedures
e) Test Procedures
f) Maintenance Plans

5. A member of the senior management team shall lead the IT disaster recovery plan.
6. Contingency procedures shall be created by the IT disaster recovery professional.
7. The IT professional is also being used for training to all employees for information security.
8. IT contingency plans shall be reviewed by the frequency of once in every 18 months.

Responsibilities:
Top Management
IT Professional Company
System Administrator