DTL ANCILLARIES

DTL ANCILLARIES LTD, CHAKAN-PUNE

Information Technology Policy

PROCESS OWNER: - IT OFFICER

Table of Contents

1. General Computer Operations Controls

1.1 Physical Security

SERVER ROOM (Head Office)

We have outsourced server Location, Mumbai with a policy of 6 months back up.

Server review:

Our network / system Engineer reviews the security & stability-Twice a week.

FIREWALL Policies:-

As recommended by the service provider firewalls are regularly updated.

Data Security

Seqrite Endpoint security Anti Virus is used both at the workstation and server levels. The virus definitions are instantly downloaded on to the server and synched simultaneously with all clients. We have a fully monitored Firewall.

Backups

Back up is undertaken on the following basis:

1. User backup on IBM server email and data (word /excel file / docs) is undertaken daily.
2. Tally data manually backup on external hard disk daily.

Disaster Recovery

In case of hardware or system failure, IT undertakes backup on a daily basis and alternative back up arrangement is in place.

1.2 Change Management

For any change in application, approval is taken from management verbally. Without approval no changes can be made to any system or application. Application changes consist of the installation of vendor upgrades, patches and customization of in-house systems / software used by ABC Limited. For major upgrades, necessary infrastructure preparations are made by the IT personnel/service providers, the upgrade is installed in the Test environment and tested by the IT/Business Users. After testing is completed, IT will migrate the same in Production environment and confirm verbally to Management / User Department.

2 System Access

Company has implemented the following Windows/network password security control:

- Password changes are forced at 45-day intervals.

A Firewall exists to control remote access activities.

Adding and removal of user system access

IT receives verbal communication to facilitate the granting and removal of user system access accounts and privileges. Access and termination requests (verbal) from the Management are processed .

Jt. MD must authorize (verbal to IT) employee system access and termination requests and forward to the IT Administrator for processing.

When a user is employed, changes job duties, or is terminated, access privileges will be granted / modified / removed to all resources as appropriate.

2.1 Software Access

When an employee joins, based on his department and position, software/applications are installed on his system.

In case, the user wants any new or additional software/applications, the user verbally informs IT department with the request. IT will verbally check with Head of Department for software installation or access as applicable.

If request is denied the user is informed verbally.

2.2 Group mail Management:

Each department and sub teams have specific folders and email ids. When an employee joins, based on his department and position, access to folder and mails is setup.

2.3 Internet policy

The site blocking is controlled based on the firewall level. In case, the user wants to access a blocked site, the user verbally informs IT department with the request, this request is confirmed with HOD for access. If request is denied the user is informed accordingly.

2.4 IT Review

Ongoing Review

The IT Administrator visually inspects the server place (generally on a daily basis) and check if all amenities like air conditioning, power supply, ups, security of servers, etc. are provided appropriately. All the firewall and servers are checked.

Bi-weekly Reviews and reviews as and when needed:

1. Check all mail related servers for space, application logs and health.
2. Check mailbox synchronization and health of mailboxes.
3. Check device management of common drives.
4. On the network level, check the internet and local loop graphs for any loss in packets or latency.
5. For any virus / malware/spyware, alert messages are scheduled on the anti-virus to be sent to the administrator email id. These messages are received and reviewed by the system administrator group.

Weekly and monthly reviews:

1. Check email and other data backups are successful. IF any error than the same is rectified and the backup is taken again.
2. The respective backups are then copied to a different server and location.

Policy Review

IT policy and procedure is reviewed as and when required to incorporate any updations / changes.