IT Policy of Harrisons Malayalam Limited

Introduction

The End Users of Harrisons Malayalam Limited, are extensively dependent on Information Technology (IT) for performing their business operations .Owing to need for rapid use of advanced communication network connecting multiple locations, implementation of Enterprise resource planning application with massive data bases , management of IT function has become significantly critical .This bring us to the moot point of we manage our IT infrastructure and application from technical obsolescence and IT security risks. It is also extremely important to bring in standardisation to IT infrastructure to sustain IT operations. Though we observe and follow certain policies and procedure in regard to upgrades & security processes, .The same need to be improved up on. This is an improved documentation of the policies and procedures related to information Technology operations.

Hardware

Personal Computing

Computing equipments like desktop/Lap Top/Ink jet Printers /MFD/DMP etc are covered under this section. The standardised configuration for procurement of P.C /Lap top is as follows

Equipment	Processor	RAM	HDD	O/S	Monitor	CD/DVD
Desk Top for ERP Data entry	C2D	1 GB	80 GB	Xp professional	TFT15"/ CRT15"	CD-ROM/Pen drive
Lap Top	C2D	2 GB	160GB	Xp professional /Vista	TFT15" / 14.1""	CD-ROM/Pen drive

Hardware specification will be reviewed every Six months to upgrade based on requirement.

Printer are taken on rental to take care of obsolesce of the hardware & to ensure cost effectiveness. All estates, Divisions &Head Office have been

provided with such printers. Network printers are encouraged to reduce the number of equipment & increased utilisation.

Owing to the dynamic work requirement, Laptop with always on Internet connection is provided to employees in management grades based on specific approval from the respective functional Heads & MD. Replacement of Laptop will be after every 3 years. All the laptops provided to the executives will be insured for domestic/international use as per requirement. All executives with the exception of VP's & MD who have been allotted company Lap top will have to surrender their desktop.

Replacement of PC for mail, Internet & office tool user would be after every five years .However if required for specific users upgrade to higher configuration will be on need basis and with the approval of V.P.(Finance)

Any variation to the above will require MD's specific.

Server -(for ERP and other applications)

The application servers will be upgraded based on the following Factor:-

- Load on the server and hence fast response.
- Scope for Scaling it up
- Version incompatibility – between application ,operating system and data base
- Support provided by Vendor – Technology obsolescence

Software –Upgrade

Application software

Centralized application like ERP will be upgraded depending on business requirement of increased functionality, Technical compatibility & the support provided by the software vendor.

Office productivity tools

We have currently standardized on Microsoft office application as office productivity tool. Upgrades of Operating system & M S office application would

be every five years depending on the circumstances prevailing from time to time.

Security

Application security, Backups & Restoration

All our application including our mail server will be hosted at Head office data centre which is secured physically through lock & key to prevent any unauthorised intrusion. Regular back up is taken at specific interval to both SAN & Tape drive. Daily E mail giving the details & status of the backup is received by the Manager (IT).Over and above this, access to applications will be controlled by specific user name & password combinations.

As far as disaster recovery is concerned, we have decided to adopt the "Cold" DR policy currently. Essentially it means that the entire back up would be taken on a different set of media & the same will be stored at a different geographical location at fixed interval.

Mail back up is provided through centralized server, while back up of all Lap top & specific users indentified by Department head is backed up in the main server. While backup of individual PC contents need to be carried out by the respective user.

Password

In order to safeguard information & computing recourse from various business and environmental threats, systems & procedures we have implemented appropriate password controls to protect business data, related application systems & operating system software from unauthorised or illegal access. To address these following steps is implemented.

- User password should remain confidential and not to be shared or otherwise disclosed to another person in any manner.
- Validity of password 60 days
- Password- should be at least 8 character.

- System controls & access rights have been defined to effectively protect ERP integrity.

For users logging into the Intranet/Mail server/applications servers other than WAN points would need access trough an extra layer of security (RSA two token) this would ensure that no unauthorised usage take place.

Virus protection

The organisation will implement procedure of It recourses (desktop/Lap top and servers) from all possible computer virus by providing the required technical support for timely distribution of antivirus software, it's updates and upgrades as well as ensure prompt reporting of virus incidents and management. The antivirus software is standardised across the organisation.

Virus protection is at two levels:

1. Centralised serve (like mail server etc) .This is addressed by installing the antivirus software at the gate way level and is managed by the IT Team.

2.Indiviual desk tops & Lap tops :Latest patch of Antivirus will be loaded on the desktop and Lap top automatically through antivirus server once the machine is connected to the network.

Checking the software downloaded from Intranet

Software/Data downloaded from outside sources such as intranet may contain virus(es) .Before such electronic contents are decompressed ,the user should always have Anti Virus software active on such computers. In order to provide more security, he should log out of all file servers and terminate all other network connections. Before executing the software, It should be screened with the approved Anti –Virus package. If a virus is detected, no further work should be carried out on the affected machine until the virus has been shown to be eradicated.

Virus reporting

In case of any virus detection, the antivirus software would act automatically. But in case of a situation where we cannot have an automatic cure, the user should shut down the system and inform the Manager (IT).

Usage.

It is expected from every It user that he/she uses the IT infrastructure only for discharging official duties and exercise due care while using the same. The following action will tantamount to gross indiscipline and will lead to disciplinary action

- Using/Copying pirated and/ or Unauthorised software
- Accessing Internet site which are illegal
- Disabling the installed antivirus software on a desktop /Laptop by the user