

## 1. Technical Support & Maintenance Strategy

Three approaches are designed to provide end-user with efficient and effective after sales technical support and maintenance of user installed equipment. These approaches are intervention at site upon receive of repair calls, intervention at workshop and laboratory if equipment are required to be taken back for further diagnosis and repair of fault. All these approaches are designed to maximize the downtime of the equipment and provided user with maximum use of their equipment.

### Intervention at site

- Replacement of the major assembly, identified by the self diagnostic and diagnostic program.
- Replacement of the miscellaneous parts that requires simple tools and easy operations.
- Tools and parts:
  - Service manual
  - Diagnostic programs
  - Entire modules
  - Miscellaneous parts
  - Tools

### Intervention in workshop

- Repair the relatively easy faults ( i.e.. keyboards, display, drives etc)
- Major mechanical repair/adjustment ( printers)
- Tools and parts:
  - Diagnostic programs
  - Spare parts
  - Technical tools

### **Intervention in Laboratory**

- Repair the electronic modules
- Tools and parts:
  - Diagnostic programs
  - Schematics
  - Repair programs
  - Spare Parts
  - Technical & Specialized tools

All the permanent faulty modules (i.e. disk enclosures), will be sent to our Vendor Factory repair. In order to ensure the available of the modules in the service center workshop, the central stock will exchange the faulty modules with a good one as soon as the service centre concerned between the workshops at service has dispatched the board. The movement of faulty modules between the workshops at the service centre and the laboratory are monitored by the central stock.

### **Diagnostic/Documentation/Spare Parts**

Having the experience of maintenance multi-vendor equipment, we have advantage of having:

- Original Spare parts
- Original modules and boards
- Repair programs
- Service manuals
- Schematics

With our experienced engineers and technicians, well equipped with the latest equipment, we are able to work in an effective manner and professional level to maintain high system availability.

### **System Downtime**

Generally, downtime is attributed to machine failure and comprises Our response time i.e. the time taken by the Field Engineers/Technician to respond to a call, and the time taken to repair, i.e. the time to rectify the machine fault so that it becomes operation again. The average total downtime would be within six (6) hours for all installations.

### **Repair time**

The average duration of a remedial duration visit is 1.5 hours. A visit involves the running of special diagnostic program, swapping faulty modules and/or mechanical alignment. When called in for technical assistance, the support specialist may provide technical advice and additional on site assistance, or recommend a total component /module replacement. Should the support specialist fail to recover the system in the specified time, escalation procedure will be put in place. Loan equipment is made available for end-user in order to minimize disruption to their daily operation.

### **Average Response Time**

The average response time is the time taken by the Our Engineer / Technician to respond to end- user call for technical assistance or repair call. The average response time is calculated from the time a repair call is receive by Our service centre nearest to the end user site and the time taken by Our reaches end-user site. These averages are calculated on a monthly basis. However there are instances when these times cannot be met due to unforeseen circumstances such as act of GOD and busy traffic conditions.

| <b>Distance from the nearest Our services centre</b> | <b>Average Response Time ( Hours)</b> |
|--|---------------------------------------|
| <b>Between 0 and 48 KM</b>                           | <b>Within 1 hours</b>                 |
| <b>Above 48 KM</b>                                   | <b>Within 5 hours</b>                 |

### **Service Performance Level Reports**

With the help of our helpdesk system, we will be able from time to time, provide the customer with the service level report. These reports encompasses down time, response time, repair time, etc. The report can be itemized to the individual piece of equipment or be presented by branch, state or site. The reports not only verify the jobs done but it can also be used to identify problematic equipment. Please refer to our standard preventive and remedial form.

## **2. Proposed nature of Infrastructure Server, Desktops and Networking Equipments for Clients Maintenance**

### **2.1 Server Maintenance**

#### **Operating System (OS)**

- To provide preventive maintenance services for all servers at clients premise. Applications systems are excluded from our proposed preventive maintenance scopes.
- To provide corrective maintenance services for all servers at clients premise.
- In some cases, we will assist clients in identifying faulty devices, justify the source of problems and forward our recommendations for further action by our client.
- Daily Maintenance task will include but not limited to monitor CPU, memory and network interface card utilizations rates. It is imperative to ensure that resource consumption for every server always within normal operating level. Therefore the first task that we will perform is to document and analyze the normal operating level of every server as our guidance and benchmarking point.
- To perform auditing for Event Viewer and relevant logs files to analyze and monitor systems activities, security and network services application logs.

## **2.2 Antivirus Maintenance**

### **OfficeScan Corporate Edition (OSCE) Server Maintenance.**

- To monitor overall client and server communications in terms of pattern update, server to client verifications, virus clean up and post attack damage clean up processes.
- To perform centralized remote administration task such like pattern update notification, damage clean up notifications, virus and firewall log consolidation.
- To provide on-site troubleshooting services such as abnormal activities identification, analyze and repair any damage caused by virus infection or system malfunctions.
- To identify any clients computer that unable to perform centralized pattern update or needed manual clean up or post attack damage clean up.
- To schedule troubleshooting task to manage identified infected and problematic clients computer.
- To analyze virus infection log, desktop firewall log and to plan for best strategy to combat malware attack by combining overall network protection agents such like the firewall, the distribution switch and also the desktop firewall.

### **Trend Micro Server Protect**

- To ensure that every contracted server will be installed with Trend Micro Server Protect and a candidate server will be chosen to host centralized management console for ease of management.
- To closely monitor and ensure that all virus patent and scan engine are updated to the latest release
- To monitor and ensure that all automated virus cleaning mechanism performed successfully, and identify any servers that needed manual intervention in cases the scan engine unable to remove the infections.

### **Trend Micro Interscan Web Security Maintenance**

- To provide transparent proxy service for HTTP, SSL and FTP traffic for the whole client's network for each internet access activities.
- To configure dedicated access policy to help preventing the users from visiting any risky web sites that may infect the computers with malware and spyware.
- To closely monitor and ensure that all virus pattern and scan engine are updated to the latest release.
- To analyze access logs and virus incident for the purpose of reporting and bandwidth utilizations.

### **Trend Micro Interscan Messaging Security Spam Prevention Solution Server Maintenance**

- To configure IMSS as the mail-based viruses protection by policy enforcement, filtering and spam removal before its reach users desktop.
- To closely monitor and ensure that all virus patent and scan engine are updated to the latest release.
- To analyze blocked email logs and virus incident for the purpose of reporting and risk mitigations.

## **2.3 Network Services Maintenance**

### **DHCP**

- To ensure that each segment having enough IP addresses allocations at all time.
- To monitor leasing statistic to ensure any problems with regards to IP Addresses quota will be resolve before it become a problem to clients networking activities.

- To configure and allocate IP Reservations for each workstations and network devices for forensic purposes should there be any incidents that need traces of sources of problems for a given time.

### **DNS**

- To provide address resolution service to network users for the purpose of accessing in-house applications and the internet.
- To ensure DNS server is correctly configured and performs as it expected.
- To take corrective actions in case where access to certain internet servers of in-house applications or peer-to-peer communications failed due to dns services error.

### **Directory Service (LDAP)**

- To monitor and ensure that directory service replications activities had been successfully carried out as per schedule.
- To manage and maintain users' accounts, publish share folders, roaming profiles and printers for end user.
- To manage and maintain group policy configurations for security application to members servers and users desktop, and also centralized WSUS servers.

## **2.4 Desktop Computer Maintenance**

To provide preventive maintenance services for all Windows XP Professional at clients computer. Applications systems are excluded from our proposed preventive maintenance scopes.

To Provide corrective maintenance services for all Windows XP Professional at clients computer. Applications systems are excluded from our proposed corrective maintenance scopes.

### **OfficeScan Client Enterprise (OSCE) antivirus client and Desktop Firewall /IDS**

- To format and reformat every single desktops in clients environment for a persist clean networking environment and benchmarking purpose.
- To configure desktop firewall and IDS protections from OSCE management console and segregate the security policy according to the users' job functions requirement.
- To provide post-attack corrective maintenance in cases where infections remedial require manual intervention at site.
- To provide preventive program which includes examination of antivirus client's functionality and desktop firewall status as per agreed schedule with the clients official.
- To provide consultation service for best practice desktop management for clients IT Team.

### **Security Policy / Group Policy**

- To provide security policy for each desktops via centralized *group policy*.
- To continuously monitor services required by each user to comply with configured security policy.

### **Security and Patches Update**

- To configure each desktops via group policy for centralize updates from Windows Security Updates Server (WSUS).
- Updates processes will be scheduled by assigning each network segment with different updates interval in order to manage traffic bandwidth in clients networking environment.

## **2.5 Switching System Maintenance**

- To provide corrective and preventive maintenance for the switching system.
- To configure switching system to form network segmentations into VLANs.
- To take full use of switches management and security features in managing virus outbreak mitigation and attack preventions.
- To ensure that at any given time, the consumption rate of the network bandwidth capacity not exceeding 37%.
- To identify any problems related to network connectivity and taking necessary remedial action to resolve it.
- To continuously monitor any security and patches update requirement and to perform the necessary upgrade should there be the need.
- To centrally monitor switching utilizations through manipulations of SNMP agents and RMON with CiscoWorks Network Management Software.
- To integrate CiscoWorks NMS output with several other network monitoring and analyzing utilities such as Sniffer PRO and SAWMILL Enterprise Log Analyzer for the purpose of bandwidth utilizations rating and throughput aggregating for future capacity building and as a parameter for network troubleshooting.

## **2.6 Router & Firewall Maintenance**

- To ensure that routing capability is working at all time, and each segment can communicate with each other as per allowable routing policy.
- To continuously audit and identify any routing requirement as well as its efficiency so that the service level is guaranteed at all time.
- To closely monitor the status of vulnerabilities reported by network security bodies in the internet and taking necessary actions to avoid and protect the router from being the sitting duck target.
- To configure the router to send syslog data to Network Management Server via netflow function for the purpose of inbound and outbound traffic flow auditing.

- To identify any host that created high volume of traffic and consume huge amount of available bandwidth and taking necessary actions to prevent it from congesting the data highway.
- To monitor and ensure WAN connection to and from clients premise is available at any time.
- To perform penetration test in order to ensure that all policy setting is perform as the intended configurations to be. Port Scanner and Vulnerability Scanner utilities will be made available on our own cost for this purpose.
- To analyze from time to time all firewall log with the usage of SAWMILL ENTERPRISE and produce inbound and outbound trend and to investigate any communications protocols that regularly causing problems in the environment.
- To monitor and inspect any attempt to over rules the configured policy setting so that any malicious means can be identified before it became the liability to the network.
- Continuously auditing and updating policy setting requirement to provide an efficient and effective firewalling system.
- To monitor all segment that connected via firewall legs.
- To provide consultation service and advice on any changes that able to increase the level of security and effeciency for the network.

## **2.7 Performance Management**

- To design Network Management Server and consolidate the placement of all network monitoring and analyzing tools such CiscoWorks NMS, Netflow System, SAWMILL ENTERPRISE Logging System and SNIFFER PRO.
- To monitor overall capacity of networking system and it subsystem.
- To prepare network capacity utilization report and prepare capacity planning plan if requested by clients official.
- Proactive monitoring and tuning.
- To measure and analyze system performance.
- To perform planned corrective program.
- To monitor application response time and aggregate throughput..

## Service Maintenance Plan, © MySepadu Systems 2010

- To proactively inform clients official before any resource reach its critical level.
- To provide corrective steps in solving capacity and performance issue. To propose and ensure no recurring problems take place.
- To prepare change management plan and its liability.
- To change any system profile if it is necessity to do so.