IT Maintenance Procedure

Red Opal Innovations

Version 1

Table of Contents

Introduction

This document outlines the procedures for undertaking hardware and software maintenance within ROI. All associated forms are available from the ROI Intranet.

Types of maintenance undertaken within ROI

The IT department undertakes the following maintenance tasks:

General maintenance

- Configure the operating system to download and install updates automatically
- Change the status of a start-up program (enabled or disabled)
- Configure Data Backup and Recovery
    - Schedule backup files incrementally on ROI servers at 9:00pm each night. This ensures that the backup doesn't affect server speed or availability during working hours
    - Before performing any systems upgrade or maintenance, a Full System Image Backup should be made by attaching an external Hard Disk (Label: SYS-Backup) to the system. This is done to ensure that the client's system can be restored in case of an upgrade failure or data corruption during the process
- Scan system for viruses
    - Configure to continuously monitor for viruses
    - Check virus signatures and definitions are up to date.

Preventative maintenance

- Defragmentation and clean-up of drives
- Installation and maintenance of anti-virus software
- Removal of malware and bloatware
- Updating software and operating systems
- Backing up files and other work-related data
- Configuration of security settings and personal firewalls
- Removal of unused software
- Cleaning/dusting of PC internals, fans and intake grills
- Inspect computer parts for damage: check computer hardware including monitor for dead pixels, fans, power supply and RAM.

Breakdown maintenance

- Maintenance of printers including the replacement of roller kits, drums, etc.
- Upgrading or replacement of hard drives, expansion cards and drivers
- Upgrading and maintenance of servers.

External maintenance

Preferred suppliers complete the following tasks externally:

- Repair of circuit boards where needed
- Repair of high voltage equipment such as power supplies and CRT monitors (now obsolete)
- Repair of digital cameras
- Repair of scanners and other peripherals.

Maintenance and diagnostic testing procedure

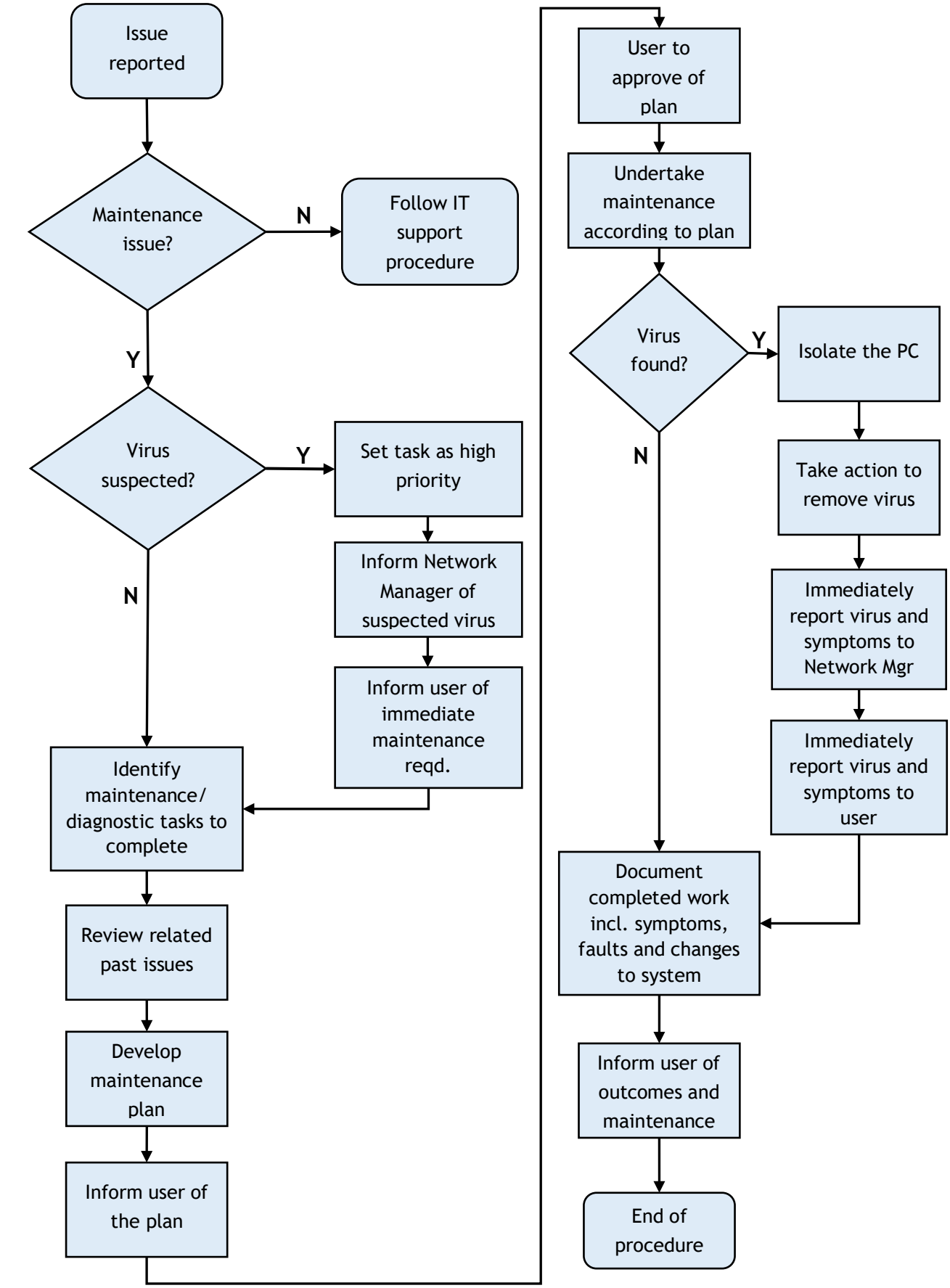
General principles:

- The Network Manager is responsible for establishing maintenance schedules in accordance with the recommendations of the suppliers.
- Before performing any maintenance, it is required that systems are fully backed up.
- Operating systems and applications software is to be kept up to date with updates and patches.
- Hardware devices are to be maintained in accordance with the manufacturer's recommendations.
- Where practical, maintenance is to be carried out in normal working hours without disruption to the operation of the company. If it is not practical, the maintenance is to be performed out of working hours in accordance with the Procedure – Technology start up and shut down.
- When maintenance or diagnostic testing is performed on IT equipment, the IT Maintenance Log must be completed. The original should be kept on site with the machine and a photocopy returned to IT Support.

The flowchart on the following page outlines the procedure that needs to be taken when an end user reports one of the following types of issues:

- Slow PC
- Random crashing/blue screen of death
- Warnings/alerts about viruses
- Pop-up ads
- Slow boot times
- Error messages when running applications.

Maintenance/diagnostic testing procedure flowchart



Maintenance plan

Once an issue has been assigned, the technician responsible needs to create a plan that prioritises maintenance tasks, outlines timeframes and proposes a contingency plan to allow staff to continue working while their regular PC is worked on.

This contingency plan can include providing a loan PC or laptop if the work is expected to take a considerable amount of time. If a virus is suspected, both the Network Manager and user need to be informed. This causes the job to be a high priority. As a part of the maintenance plan, a virus scan must be run prior to any other scans.

Viruses

If at any time a virus is found on a PC or server, the machine must be immediately isolated. Unplugging the network cable and ensuring that the machine is not used in any way will achieve this. The virus can then be removed and the entire machine scanned for other malware.

Reporting viruses

Once the above steps have been taken, the Network Manager must then be informed about the virus via email. This email will include the virus name, its symptoms and the steps needed to remove the virus. Reporting any viruses found allows the Network Manager to inform other IT staff, alert all ROI staff to the danger and co-ordinate a response to the virus threat.

The staff member using the PC that the virus was found on will also need to be informed so that they can scan additional files that might be saved on USB drives or taken home. By informing the end user of the virus, further information about how the PC was infected can be obtained, and training can be provided to protect against future infections.

Maintenance schedules

Maintenance schedules should be created and adhered to for all IT equipment, including associated peripherals. Manufacturer recommendations for maintenance of equipment should be followed.

Moving, locating and storing equipment

Manufacturer recommendations should be followed when moving and storing any equipment. If manufacturer recommendations are not available, then ensure that WHS procedures are followed, and environmental considerations such as temperature, dust, ventilation, humidity and vibration are accounted for.

ROI is currently located in an area that has many electric power surges and electricity restrictions. Computer equipment must also be protected from these electrical issues appropriately.