

## Daily

1. Automated backup of essential user, application and relevant system files
2. Automated update of virus definition files for relevant software

## Weekly

1. Review server error logs and reports
2. Check the storage device statistics and permissions
3. Review file server cache statistics
4. Review server disks and volumes

## Monthly

1. Review all users and objects on the network ensuring that there are no unauthorized accounts, file tampering, improper services and improper use of services and systems.
2. Review and ensure that backup devices are working correctly
3. Update security patches at the OS and application level
4. Provide any pre-requested support items or configuration amendments that have not been deemed urgent but agreed upon to take place upon set date.

## Twice a Year

1. Ensure Uninterruptible Power Supply (UPS)(if available) is functioning suitably.
2. Detailed and concise technical analysis of server performance, suitability and recommendations.