Standard Operational Procedure (SOP)

1. Schedule a daily backup of system data and verify on Backup server
    GUI >> System Configuration >> Manage Data >> Set Backup Schedule
    (For System as well as Web surfing logs)
    Note*: Configure schedule backup on external FTP server and monitor regularly. Need to verify backup size and check internal data at regular period of time

2. Auto purge 'Deactivate Guest User' to be set.
    GUI >> System Configuration >> Manage Data >> Configure Auto Purge >> Purge Guest Deactive Since
    Note*: Recommend 60/90 days

3. Service monitoring should be done at regular intervals.
    GUI >> System Configuration >> Services

4. DoS settings should be verified for any type of External attack protection.
    GUI >> System Configuration >> Firewall >> DoS Settings
    Note*: 12,000 packets is the standard default value for Sync/UDP Flood
    UDP ports 2812,2813 and 53 should be bypassed in Dos Bypass if we apply DoS settings for Udp traffic.

5. Ping Gateway IP and check gateway status at regular interval.

6. Regularly monitor Audit logs.

7. IP Configuration: Need to make changes at all three location
    1. **Need to create IP Pool: GUI >> Property Management >> Manage Pool >> Create Pool**
    2. **DHCP Configuration: GUI >> Config Tab >> DHCP Configuration >> Add Subnet and Pool**
    3. **Need to make change in VLAN configuration on L3 Switch**
    4. **Advance Network Settings entry should be configured for LAN pool in order to get captive portal   and bandwidth control/allocation to work properly as it is required to fulfil 24Online architecture.**

8. Websurfing Logs & Net Kapture Logs must be stored on External Device. If local storage of web logger is there than purge the logs every two weeks after Backup Verification to avoid database and server performance related issues.

9. All upgradation should be done only after reading and understanding Release Note. End customer understanding of the same should be confirmed before upgrade.

10. Before doing any kind of network related changes or configuration changes end customer has to consult vendor / partner technical team and need to inform them what kind of changes they are willing to do in the network over mail in written record in order to avoid any communication gap, so that necessary corrections can be taken in advance to avoid any chances of misconfiguration.

11. The person from customer or partner side who configures different policies, packages and other configurations on 24Online should have clear and proper understanding of his requirement and should be able to communicate with support team to explain his requirement to have proper assistance.

12   All accessories of Appliance to be kept safely and handy so that serial console cable or any other thing is required then it can be used immediately.

13.   Zero Configuration Pool should be default Pool and with default Pool Captive portal should be page, not url based captive portal.

14.   Regularly monitor audit log reports and Web Surfing Reports for security purpose.

15.   Standby Appliance should be kept ready on same software version for redundancy purpose so in case of hardware failure of Live Server, latest data can be restored on Standby server to make it live. This will help to reduce downtime in case of hardware failure.

16.   Auto Backup must be verified everyday and repository must be maintained. In case of export to FTP Server.

17.   Customer has to keep track record of special customisations developed for his own server and need to verify its functionality after each version upgrade and need to confirm working status to support team. Below are the customizations which needs to be taken care

   On RADIUS:
   1. HA   High Availability
   2. HTTP MAC
   3. MAC based Dynamic Users
   4. Change Window Title

   On NAS:
   1. HA   High Availability
   2. HTTP MAC
   3. MAC based Dynamic Users
   4. Change Window Title

18.   User session log, Audit log and deactivated users need to be purged on regular interval.

19.   Latency to the gateway should be 1-2 ms or less than 1 ms.

20.   Service monitoring should be done at regular intervals under System Configuration >> Services on GUI.

21.   Data Maintenance Activity must be done at least once in a year. To do so please contact 24online Support Team.

22.   User Sessions must be removed older than 1 year for Active Users and older than 3 months for deactivated users after Backup Verification.

23.   Auto Backup must be verified everyday and repository must be maintained. In case of export to FTP Server, FTP server maintenance should be done every week at least.

24.   PIN, Audit Logs and deactivated users needs to be purge on regular interval.

25.   Standby Appliance should be kept ready on same software version for redundancy purpose so in case of hardware failure of Live Server, latest data can be restored on Standby server to make it live. This will help to reduce downtime in case of hardware failure.

26.   If DHCP server is running on 24Online server then there should not be any other DHCP server in the same network segment.

27.   Whenever it is required to reboot the 24Online server, always do soft reboot. It is strongly not recommended to do hard boot of the server to maintain longer life of server hardware.

28.   It requires to configure external SMTP mail server if mail alert is required to be configured.