Compliance Procedure

Title: nGenius Monitoring and Startup Procedure
Reference Number: 9.3.2.2B

Purpose

The purpose of this compliance procedure is to define the procedure to start network monitoring via the nGenius network monitoring application and to identify the response processes needed by Operations staff to deal with any alarm resulting from the monitoring.

The intent is to ensure standard response actions in identifying alarms and reacting to alarms are known to the entire staff and issues are addressed with consistency.

Procedures & Related Information:

OCCS Operations shall utilize the network monitoring application entitled nGenius as one of it’s prime monitoring tools on all shifts.

Operations supervisory staff shall set up automated testing scripts via nGenius to monitor/exercise essential servers and essential server applications to execute at 5 and 10 minute intervals so as to ensure such services are active and available.

Such tests shall generate exception alarms upon a failure of an automated test of a key service.

Failures will appear on the nGenius Performance Manager Console screen for visual inspection and analysis. Failures will also alarm on the Operations pager device to serve as an audible alarm for Operations attention.

Errors/Alarms/Failures shall also be sent as emails to the entire Operations staff for processing and historical records.

All alarms for Operations attention shall begin with the words “OPS – Test for ....” So as to further identify themselves for processing and analysis.

Operations staff should approach supervision for the proper Account ID and password to achieve login. The nGenius product application for Operations usage is bookmarked on Internet Explorer. The necessary IP address for the application is 192.168.5.24.

Start Up Instruction for nGenius application:

At the console:

- Click on "Ngenius Client" Icon.....on screen
- Click on Connect
- Log in
- Account ID is "operations"
- See supervision for the password – passwords will not be written down
- Staff will soon utilize their own sign on – we will move away from communal accounts
nGenius will load up the screen – in the center under NGenius Performance Manager section.....go to "Workspaces" - click on Workspaces.
That will bring up the Performance Manager screen.....and you should be in Workspace1
Click on "View" - then "Alarm Viewer"
This will open up the Alarm Viewer - you want to be under "Power Alarms"
Go to the Clock on the right of the 2nd level toolbar.....
Click on the clock and select "real-time"

At that point, all new messages will come up.....from there – interpret all alarms based on the procedures, the alarm response log and what you have been shown......ALL alarms are to be logged in our book and investigated.

**Alarm and Response Procedures:**

Upon getting an alarm/error/failure, the console operator must determine what has failed and whether support staff needs to be called. Once that determination has been made, the appropriate support group should be called.

The proper procedure for these actions is:

- Recognize the server/application name identified in the alarm message
- Document the alarm event in the Ops Log book
- Reference the server name in the Server Function List to determine the likely area of impact on the campus community
- Reference the Response Procedures Documentation to determine what actions to take and what support group will likely be involved in the resolution
- Prior to calling support teams, review the ProdChng event notices to ensure that the device is not available on purpose/planned
- Check the Backup Schedule to ensure that a device is down due to it’s being backed up
- Call support team utilizing the On Call calendar – should that person not respond immediately, call another staff member in that group or group supervision

After prime work hours and on weekends, all of the above steps should be utilized. Due to large availability of staffing, it is likely that not all steps need to be executed.

The actions of calling support teams and resulting resolution should be documented in the Ops Log should be done by every shift.

**Definitions**
OCCS is the acronym for the official name of the Office of Computing and Communications Services.

### Policy References

ODU faculty, staff and students are bound by all applicable laws, policies, standards and procedures and guidelines. For reference, some frequently referenced documents are noted. This is a non-inclusive list and not intended to limit applicability of any other law or policy.

| Policy Foundation: | Federal and State Law  
<table>
<thead>
<tr>
<th></th>
<th>Policy 3507 Operations Management</th>
</tr>
</thead>
</table>
| Related Standards: | IT System and Data Backup and Restoration Standard  
|                    | Server Management Standard  
|                    | Network Management Standard  
|                    | Change Management Standard  
|                    | Print Management Standard  
|                    | Physical Security Standard |
| Related Procedures, Forms: | System Monitoring procedure  
|                           | Console Logging Procedure  
|                           | Customer Notification Procedures  
|                           | Alert Posting Procedure |
| Related Guidelines: | System Monitoring Tips  
|                    | Call Out List  
|                    | Customer Contact List |
| Maintenance: | Office of Computing and Communications Services |
| Effective Date: | Reviewed on an annual basis |
| Approved by: | Rusty Waterfield  
|               | Acting Assistant Vice President, Office of Computing and Communications Services |