Compliance Procedure

Title: **Monitoring & Problem Escalation Procedure**
Reference Number: **9.3.2.2A**
Revised: 3/2010

Purpose

The purpose of this compliance procedure is to define the procedure in place with regard to identifying system/network issues, escalating issues to support teams and effective communications regarding problem determination and resolution. The intent is to have a process in place that deals in unison with our monitoring tools to best utilize staff time to optimally provide essential services.

OCCS utilizes multiple automated enterprise software products to provide dynamic monitoring and notification to the duty operations staff and support teams when applications response times exceed defined limits. Successful monitoring is a summation of such software notifications and proper response by duty staff.

These automated monitoring products act separately to monitor network hardware, essential applications and databases, on a 24x7 basis. As these products are active around the clock, OCCS has established an “On Call Calendar”, which defines what technical staff member is responsible for support in the various areas.

This On Call Calendar is used to determine the personnel resource responsible for any issues regarding problem determination and resolution. Such a system of rotating responsibility has proven successful in keeping fresh manpower and equal skill levels available to handle support calls.

Duty operations staff are expected to be attentive to capture the alarm from the software products, do some testing/verification of the alarm, interpret which support group should be contacted, based on the Action/Response List, contact the support team on call, log their actions and stand by to assist in the recovery.

Support staff will analyze instances of failure brought to their attention to determine current system health. Frequent identical failures and alarms observed by operations and monitoring software will be discussed with support staff to determine if such a problem requires intervention by additional support groups or implementation or change of business procedures. It is presumed that such monitoring should produce a true representation of error and that optimally, less alarms is the goal. With that premise, all alarms and resulting circumstances shall be reviewed so as to determine that alarms represent true problem situations and thus address them to eliminate the sources.

The following procedures and guidelines apply regarding Network and Application Monitoring and addressing abnormalities.

Procedures & Related Information

OCCS currently utilizes the following tools to do monitoring:

- Nagios
- Solar Winds
- Footprints
- Direct application execution

Each tool has a specific purpose in the monitoring process. Some deliver a visual screen to the console command station that serves a focal point for the duty Operations staff member. All operations staff are to be familiar with each of these tools. Lack of knowledge about these tools will not change the expectation that these procedures will be followed correctly and completely.

Each tool is different in terms of what it delivers to the duty operator. It is incumbent upon the operator to pay attention to the screens and delivered data. Correct operator action is necessary for our systems to be successful. Contacting the proper support staff on the first call is essential.

Problem Identification –

It is important that problems be identified as early as possible so that corrective action can be started as soon as possible. Close concurrent monitoring of the various tools can provide early warning signs of problems 'in the making'. Monitoring is to be an 'Active' process where you are actively searching for problems, not waiting for one to land in your lap.

Inputs to the Problem Identification process are:

- Nagios
- Solar Winds
- Footprints
- Direct Application tests
- Observations

Events/Alarms from these tools provide evidence of a potential problem that should be investigated and confirmed.

Outputs from the Problem Identification process may be:

- Footprint tickets
- Operator Logbook entries
- Confirmed Problems

Nagios –

Nagios is the primary monitoring tool. Warnings and alerts are displayed here. The main screens to be watched are the '**Service Problems**' screen and the '**Event Log**' screen. The '**Service Problems**' screen will identify any host/services that are experiencing a problem at the current time. The '**Event Log**' screen will show any alerts that have occurred in the past. The 'Event Log' should be reviewed, at a minimum, at the beginning of each Operators shift to see what has happened over the past 24 hours. An hourly review could show short duration warnings that have been missed.

Warning (yellow) alerts should be investigated and watched closely. No escalation or Footprints should be generated unless the investigation shows that a more serious problem exists.

Failure alerts and Notifications (Red) are a good indicator that a problem with a host/service exists. Verification should be done, if possible, by use of the other monitoring tools.

If a host or service is 'Silenced', then a comment must be placed in Nagios on the host/service that was silenced. When the host/service is un-silenced, the comment can be removed.

Solar Winds –

Solar Winds can provide information about network problems. It does NOT monitor host or applications, just network devices. It displays campus maps with green/ yellow/ red icons to represent the status of the network in the various locations on the network. Red and Yellow icons should be investigated further. Drilling down through the alerting icons can provide more and more detail about what is happening in the network. Network problems typically result in some impact upon the services monitored in Nagios.

Footprints –

Footprints should be monitored so that you can be aware of the kinds of problems that are being reported by the end users. Seeing several issues related to the same service/application may trigger a closer look at that service/application for potential problems. As the other monitoring tools indicate a problem, seeing footprint tickets will confirm that it is, in fact, having an impact upon the end users. The main screen in Footprints to be watched is the '**ACTIVE**' problems view. This will identify all 'Active' problems regardless of the topic or who they are assigned to.

Direct Application Tests –

If one of the automated tools identifies a potential problem, you should attempt to verify the problem by running the application yourself. Several attempts should be made, even if the first attempt works normally. Some errors are intermittent and only show up every 'x' number of attempts.

Examples:

- If a tool says that a web site is not available, try to access it yourself.
- If there is a problem with Blackboard, try to log into blackboard yourself.

The results of this independent testing should be noted in the Footprints ticket on the problem. Be specific as to exactly what tests were performed. This is valuable information to the support staff.

Operator Logbook –

All staff working in the OCCS Operations Center should notate the Operations Logbook at the beginning and at the end of their shift. All problems and 'events of note' must be recorded in the Operator Logbook in the chronological order that they occur. If a Footprints ticket is generated on an event, record the Footprints ticket number in the Operations Logbook with the event.

Write clearly so that anyone can read it without error. Note the time for each event recorded.

Response to Problems –

Knowing about a problem is not enough; some action must be taken to communicate about the problem and to resolve the problem. If you have the resources to resolve the problem yourself, then do so. If you can not solve the problem yourself then begin the appropriate process of getting it in the hands of someone that can resolve the problem.

Inputs to the Response process are:

- Information from the 'Problem Identification' process
- On-Call Calendar (both on-line and hard copy)
- Operator Response Book

Outputs from the 'Response' process may be:

- Footprints tickets (new or updated)
- Contact with Support staff
- Posting of OCCS Alerts
- Corrective Actions taken

Nagios –

Failure alerts and Notifications (Red) should be notated in the Operations Logbook and a Footprints ticket should be generated so that the problem can be assigned and tracked all the way through resolution.

Warning alerts (Yellow) that clear themselves after a short time should also be recorded in the Operations Logbook and a 'Nagios Warning' footprints ticket should be generated. After a Warning/Yellow alert remains active for a period of time, it may change to a failure (Red) alert. Only open a Footprints ticket for the most critical state (Red), not two footprint tickets (one for Red, one for Yellow).

Footprints –

Once a problem has been identified and confirmed, a Footprints ticket must be opened about the problem, If the problem is impacting more than one or two users, then the problem should be a 'Global' ticket. Nagios 'Warning' alerts that are not impacting the end users should 'Not' be 'Global' tickets.

It is possible that a ticket has already been opened by the TSC (Technical Support Center) or by some other party. If a ticket is already open, then it can be updated with status information that you have on the issue.

The title of the Footprints ticket should include the server and service names that have the problem. A problem ticket should be assigned to the group/groups based upon the support staff identified to support that host/application/device. This information usually comes from the 'On-Call Calendar'. Record all attempts to contact support staff in the Footprints ticket. When a support person is notified about a problem, tell them the Footprints ticket number associated with the problem and also record the notification in the Footprints ticket.

A problem ticket begins with a status of 'Open'. Once the problem is being worked by somebody, the status should be changed to 'Pending' by the person working the ticket. The person that resolves the problem is responsible for changing the status of the ticket to 'Closed'.

On coming Operations staff shall review all Footprints Tickets with the prior shift to ensure proper information is being exchanged between shifts, current status of open problems is exchanged and that new duty staff members are aware of open problems.

Departing Operations staff shall document which Footprints Ticket numbers are open at the end of their shifts as part of proper turnover procedures.

Duty Operations Staff at the time of the successful resolution of an issue shall print the entire related Footprint Ticket for inclusion/reference in the operator logbook.

Operator Response Book –

When a failure of some kind occurs, look up information about the failed host/service/application/device in the Operator Response Book. Initiate the response called for in the book.

Use good judgment and your experience when evaluating the response. If a service always 'warns' at 2AM each day, there is no need to take follow-up action when it warns at 2AM this morning. Failure of a large number of host/services at once may indicate a network problem, not that all of the host failed at once.

On-Call Calendar –

An On-Call Calendar is maintained to identify the specific people that are charged with supporting the device/application on any specific day. This calendar should be available both on-line and in hard copy (incase of hardware failure). This calendar should be referenced to know who to contact and how to contact them.

Contacting Support Staff –

When support staff are required to correct a problem, contact them via the method listed first on the On-Call calendar. If you have received no response in 5 minutes, attempt to make contact using the alternate methods listed for that person on the On-Call calendar. If no contact has been made after 15 minutes, attempt to contact the support person's manager. Keep moving up the organizational hierarchy in 15 minute intervals until the Assoc VP for OCCS has been contacted. Record each attempt in the footprints ticket about the problem.

Once a support person has been reached, communicate the Footprints ticket number and any other information about the problem that you have. The support staff should communicate to you if they will be working on the problem from remote or if they are headed on-site, with an estimated time of arrival. Record this information in the Footprints ticket.

Operations center should notify the on call person responsible for the system being reported ONE time. No more than once per open incident in any 8 hour shift. When an incident is claimed as resolved, a subsequent failure will initiate a new call to support engineers.

Continue to monitor the problem and provide any assistance that the support person needs.

Support Staff Actions –

The support staff should:

- Investigate and confirm the problem.
- Response to the operations center immediately or thereafter on the status of the failing system and any issues that were found.
- Notifying the TSC via email or phone call with the follow up information.
- Post an OCCS Alert about an the outage
- Call back to operations with periodic status reports as to what stage the problem resolution is being performed
- Resolve the problem if possible
- Post an 'All Clear' OCCS Alert if appropriate
- Update and close the Footprints ticket
- Communicate back to Operations on the status and any further instructions concerning monitoring & notifications.

Follow-up Process –

Operations Management staff will follow-up on activities that have occurred over the past day or weekend to ensure that issues are being properly addressed and that proper procedures were followed. Outstanding footprints tickets generated by the Operations staff that were a 'Warning / FYI' nature should be closed unless some response is expected from the support staff.

Failures by staff to follow proper procedures will be documented and addressed to ensure proper performance in the future.

Review of backups, alerts, footprints tickets, Operations Log and e-mails will be used to monitor the performance of the Operations Monitoring and Problem Escalation process. There is an expectation that we have an explanation for all outages. Input from support staff is required to achieve this expectation so accountability is expected.

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 Policy 3507 Operations Management
🗗 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
✓ Approved:	University Advisory Council on Technology ☒ Required for Standard