Vulnerability Management Policy

April 13th, 2015

1.0 SUMMARY

Vulnerability management is the processes and technologies that an organization utilizes to identify, assess, and remediate information technology (IT) vulnerabilities, weaknesses, or exposures in IT resources or processes that may lead to a security or business risk. This policy identifies the University of Maryland Center for Environmental Science's vulnerability management practice which includes the roles and responsibility of personnel, the vulnerability management process and procedures followed, and the risk assessment and prioritization of vulnerabilities.

2.0 ROLES AND RESPONSIBILITY

The CIO of UMCES is responsible for IT vulnerability management. The following are the key roles and their responsibilities:

Network / Server Analyst Role - Maintain inventory of IT assets. Identifies vulnerabilities via vulnerability scanning, patch releases, configuration review, and compliances. Performs remediation of vulnerabilities as directed.

IT Director Role - Determines remediation of vulnerabilities and delegates corrective action. Report any unresolvable vulnerability to CIO.

Chief Information Officer (CIO) Role - Approves any risk acceptance, emergency CMRs, and final report of quarterly scans.

3.0 INDIVIDUAL LOCATION ROLES AND RESPONSIBILITIES

Horn Point Laboratory / Central Administration

Network / Server Analyst Role:	Jason Beveridge
IT Director Role:	Kurt Florez
CIO Role (UMCES):	Kurt Florez

Institute of Marine and Environmental Technology

Network / Server Analyst Role:	Jason Beveridge
IT Director Role:	Kurt Florez

Maryland Sea Grant

Network / Server Analyst Role:	Dan Jacobs
IT Director Role:	Dan Jacobs

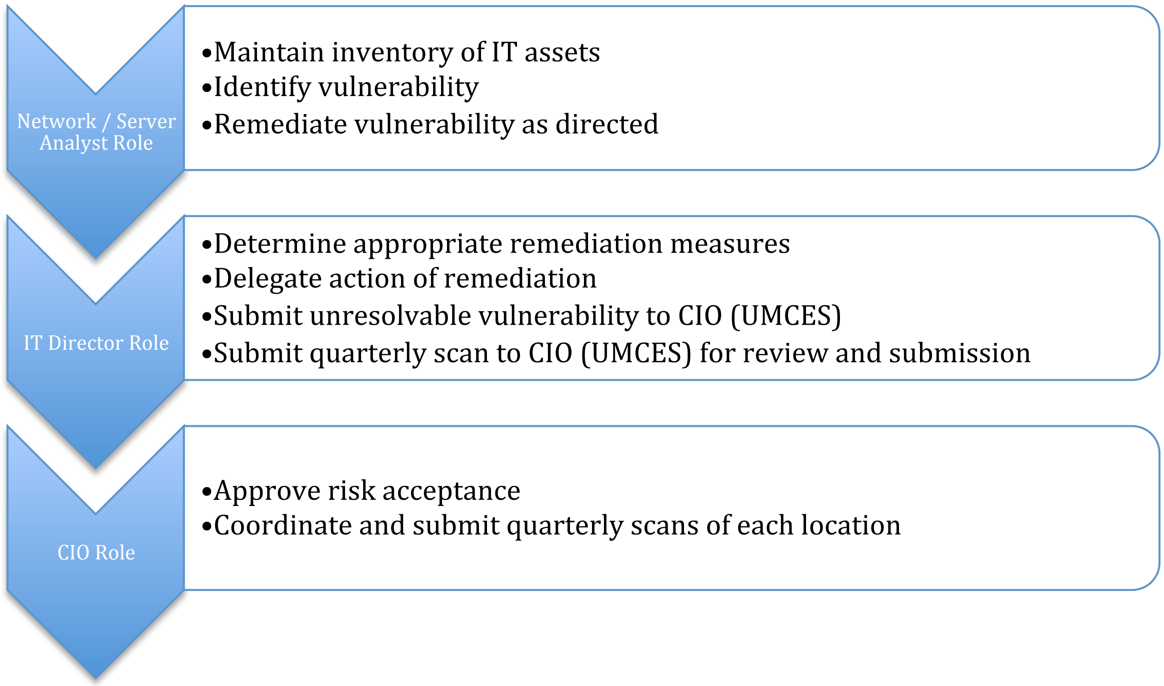
Chesapeake Biological Laboratory

Network / Server Analyst Role:	Larry Lentner
IT Director Role:	Michael Santangelo

Appalachian Laboratory

Network / Server Analyst Role:	Eric Farris
IT Director Role:	Eric Farris

4.0 FLOWCHART OF ROLES AND RESPONSIBILITIES



Network / Server Analyst Role

- Maintain inventory of IT assets
- Identify vulnerability
- Remediate vulnerability as directed

IT Director Role

- Determine appropriate remediation measures
- Delegate action of remediation
- Submit unresolvable vulnerability to CIO (UMCES)
- Submit quarterly scan to CIO (UMCES) for review and submission

CIO Role

- Approve risk acceptance
- Coordinate and submit quarterly scans of each location

5.0 VULNERABILITY MANAGEMENT PROCESS AND PROCEDURES

IT goes through a continuous cycle of scanning and remediating vulnerabilities through a series of quarterly system and network scans, configuration templates and checklists, and adhering to best practice when implementing new business solutions. Scheduled scans align with the University Systems of Maryland (USM) quarterly vulnerability requirements. Targeted system scans are adhoc or based on project requirements and timing.

Procedures associated with the vulnerability management process include:

Scan business functioning IT subnets for vulnerabilities – Networks in which systems that are vital to the business (i.e., critical systems) at UMCES are scanned. The whole subnet is scanned against a single baseline vulnerability policy.

Validate findings from scan and assess risk to IT environment – Once scanning is complete the results are verified by the network/server manager. This is done by negating false positives, (i.e., windows vulnerability on a unix system) or taking additional steps via penetration testing to validate the exposure.

Inform management for a response of action – Results from the scan are sent by the network/server manager to the CIO with a deadline of response. The manager works with their staff to schedule the work to resolve the vulnerability and provides a response of a plan of action to the analyst for the quarterly report. Critical vulnerabilities with immediate impact are expedited as emergency CMR.

Schedule an Emergency CMR – Emergency CMs are implementing within 48 hours with CIO approval.

Schedule a standard CMR - Standard CMs occur with a 2 week delay in implementation to allow business planning during the maintenance window.

Build, Test, and implement vulnerability resolution – Once a CM is approved the respective area proceeds with implementation. Testing may occur before-hand if a test/development environment is available.

Conduct post implementation scan to verify resolution – Once the change is implemented the analyst rescans for the vulnerability to verify the resolution. If the vulnerability is still present another solution may be attempted or alternative compensating controls but in the event there is no solution it becomes a risk that would need to be accepted by the CIO.

6.0 RISK ASSESSMENT AND PRIORITIZATION

UMCES currently uses the Common Vulnerability Scoring System (*CVSS*) for all Common Vulnerabilities and Exposures (CVE) provided by the National Vulnerability Database. Scoring for non-CVE vulnerabilities is provided by UB's vulnerability scanning tool. A priority is placed on patching or mitigating the vulnerability based on these scores and the logical location of the vulnerability within UMCES's network infrastructure. Remediation occurs within 10 business days for critical vulnerabilities. UMCES also documents patches to critical systems via a CMR.

Severity is assigned to vulnerabilities by the exposure to the attack vector and the risk to the IT environment. Based from the scanning software, the logical location of the vulnerability and current activity of the exploited; the vulnerability is given one of two ratings. A critical rating is given to the vulnerability if it is activity being exploited (a known exploit is public) and there is no current mitigation within the IT environment. A high rating is given if the vulnerability is not being exploited and mitigation is in place lessening the immediate risk. High severity vulnerabilities are addressed within 30 business days. (**Table 1.**)

Table 1. Shows the rating UMCES uses for vulnerabilities and the remediation time.

Severity	Description	Remediation Time Frame
Critical	Activity being exploited (a known exploit is public) and there is no mitigation the priority is critical.	10 business days
High	If it is not being exploited and mitigation is in place the priority is high.	30 business days

7.0 EFFECTIVENESS MONITORING

In order to ensure the effectiveness of the Vulnerability Management Policy, the CIO will conduct a monthly scan and create an update report. This report will collect information and maintain a status per month. The information collected will include the following categories as shown in Table 2 below: Total Systems, Systems w/ Critical Vulnerabilities, Resolved within 30 days, Repeat – Can't Mitigate or Accept Risk and New Systems w/ Critical Vulnerabilities.

(Table 2)

Monthly Scan Reports

	January	February
Total Systems	437	437
Systems w/ Critical Vulnerabilities	5	5
Resolved within 30 days		
Repeat - Can't Mitigate or Accept Risk		5
New Systems w/ Critical Vulnerabilities		

8.0 METRICS

Metrics must provide relevant and supportive information to have value. Currently, IT reports vulnerability metrics to the USM quarterly.

Version History

1.0 – Initial Draft. Kurt Florez. 4/13/15