Security Audit Questionnaire

1. Does Bukidnon State University have cyber security policies, procedures, and standards based on industry standards?
2. Does Bukidnon State University protect sensitive information received from a third-party firm during transmission between the owning third-party as well as other parties with whom that data is shared (i.e. Encryption, SSL/TLS connections)?
3. Are all devices that store or process a third-party firm's sensitive information protected from the Internet by a firewall?
4. Does Bukidnon State University have designated Cyber-security personnel?
5. Does Bukidnon State University have a cyber-security user education and awareness program?
6. Does Bukidnon State University perform cyber security audits by external 3rd parties at least annually?
7. Do all devices that store or process sensitive information utilize antimalware software with current signature files?
8. Do users that can access devices that store or process sensitive information have a unique user name and complex password to access the system?
9. Do all devices that store or process sensitive information at a minimum have access control that is configured on a least privilege model (a person only has access to the data/device that they need)?
10. Do all devices that store or process sensitive information at a minimum have vulnerability scanning performed at least monthly?
11. Are vulnerabilities being remediated in a risk-based priority (highest priority vulnerabilities are fixed first)?
12. Do all devices that store or process sensitive information at a minimum have all unnecessary ports and services disabled and the device is used for limited functions (ex. A device acting solely as a file server vs. a file server, FTP server, and web server)?
13. Do all devices that store or process sensitive information at a minimum have patches deployed for high-risk operating system and third-party application vulnerabilities within industry best practices (i.e. 48 hours) and medium/low risk patches to be deployed in <= 30 days?
14. Are all laptop devices that store sensitive information encrypted?
15. Do all mobile devices (e.g. smartphones, tablets) that store sensitive information at a minimum have configuration management provided by a firm owned centrally managed infrastructure including the ability to remote wipe the device?
16. Do all mobile devices (e.g. smartphones, tablets) that store sensitive information at a minimum have access control to the device (complex password to access device)?
17. Does Bukidnon State University have a Computer Incident Response Team (CIRT) with a formal process to respond to cyberattacks?
18. When Bukidnon State University must share sensitive information with other companies, do they require those companies to follow policies, and procedures for cyber security based on industry standards?
19. Does Bukidnon State University require 2-factor authentication for remote access (e.g. token used in addition to a username and password for VPN login)?
20. Does Bukidnon State University perform industry standard logging and monitoring on devices that store or process sensitive information?
21. Does Bukidnon State University control web access based on the risk (e.g. reputation, content, and security) of the sites being visited (e.g. Web Proxy Controls)?
22. Does Bukidnon State University have capabilities of detecting and blocking malicious e-mail prior to delivery to the end user?
23. Does Bukidnon State University actively participate in a cyber-intel sharing forum? (e.g. ISAC, Infraguard)
24. Does Bukidnon State University perform phishing e-mail testing of its employees?

Project Manager:

KHENT MARK J. DAHAY