INFORMATION ASSURANCE AND SECURITY AUDIT OF
DIGITAL INFORMATION OFFICE
CENTRAL MINDANAO UNIVERSITY

AUDIT QUESTIONNAIRE

Name of Respondent: ______________________________

Office Position/s: ______________________________

Evaluation Instruction:

Read the statement carefully, circle the number which you think is the weight of the statement.

Scale	Equivalent
5	Excellent
4	Very good and relevant
3	Good
2	Somewhat relevant
1	Irrelevant

No.	Items	Scale				
1	How well does the DTO in Central Mindanao University follow industry standards with regards cyber security policies, procedures, and standards based on industry standards	5	4	3	2	1
2	To what extent does the DTO protect sensitive information received from a third- as well as other parties with whom that data is shared (i.e. Encryption, SSL/TLS connections)?party firm during transmission between the owning third-party	5	4	3	2	1
3	How effectively are all devices within the DTO that store or process a third-party firm's sensitive information protected from the Internet by a firewall?	5	4	3	2	1
4	In terms of relevance and effectiveness, how well-defined are the roles of designated Cyber-security personnel within the DTO	5	4	3	2	1
5	How consistent and relevant is the cyber-security user education and awareness program conducted by the DTO or other relevant departments within the university	5	4	3	2	1
6	How relevant is the performance of cyber-security audits by external 3rd parties by the DTO	5	4	3	2	1
7	How effectively do all devices within the DTO that store or process sensitive information utilize anti-malware software with current signature Files	5	4	3	2	1
8	In terms of relevance, do users that can access devices that store or process sensitive information have a unique user name and complex password to access the system	5	4	3	2	1
9	In terms of relevance, do all devices within the DTO 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)?	5	4	3	2	1
10	How effectively is the performance of the vulnerability scans on all the devices that store or process sensitive information within the DTO	5	4	3	2	1
11	How well are the vulnerabilities being remediated in a risk based priority manner within the DTO	5	4	3	2	1
12	How relevant is the configuration of all devices that store or process sensitive information to have all unnecessary ports and services disabled and are they used for limited functions	5	4	3	2	1

13	How promptly are patches deployed for high-risk operating system and third-party application vulnerabilities on all devices storing or processing sensitive information, in accordance with industry best practices (i.e., within 48 hours), and medium/low-risk patches within <= 30 days	5	4	3	2	1
14	How well encrypted is the sensitive information stored in all computer devices within the DTO	5	4	3	2	1
15	To what extent do all mobile devices (e.g., smartphones, tablets) storing sensitive information have configuration management provided by the DTO centrally managed infrastructure, including the ability to remote wipe the device	5	4	3	2	1
16	To what degree do all mobile devices in the DTO that store sensitive information at a minimum have access control to the device	5	4	3	2	1
17	How skilfully is the DTO Computer Incident Response Team (CIRT) with a formal process to respond to cyber-attacks?	5	4	3	2	1
18	When you must share sensitive information with other companies, do you require those companies to follow policies, and procedures for cyber security based on industry standards?	5	4	3	2	1
19	Does the DTO require 2-factor authentication for remote access (e.g. token used in addition to a username and password for VPN login)?	5	4	3	2	1
20	Does the DTO perform industry standard logging and monitoring on devices that store or process sensitive information?	5	4	3	2	1
21	Does the DTO control web access based on the risk (e.g. reputation, content, and security) of the sites being visited (e.g. Web Proxy Controls)?	5	4	3	2	1
22	How effectively does the capabilities of the DTO of detecting and blocking malicious e-mail prior to delivery to the end user?	5	4	3	2	1
23	Does the DTO actively participate in a cyber-intel sharing forum	5	4	3	2	1
24	How often does the DTO perform phishing email testing of its employees	5	4	3	2	1