Cybersecurity

Division of the University: Academic Affairs

Administrative Unit Assessment Year Reporting: FY22 (July 2021 – June 2022)

Department and Assessment Report Information Prepared on:

Prepared by: joel.morgan@mga.edu

Email address of person responsible for this report: Joel Morgan, joel.morgan@mga.edu

Department Mission and Goals. The mission and goals of the department should be consistent over a 5-year period, although some institutional changes may necessitate and prompt a change in mission or goals for specific departments. In this section, you will report the mission statement for your department as well as the long-term goals (5-year range) for the department.

6. What is the mission statement for this department/area? Your mission should explain why the department/area exists and who it serves.	Implement and manage Middle Georgia State University's cybersecurity program and services and lead the development and execution of the organization's cybersecurity program.

7. What are the goals for this department? These should be the "big things" the department/area intends to accomplish within 5 years.	Improve the risk assessment process Improve configuration management Improve endpoint protection Improve Cybersecurity Awareness Modernize the wireless network Increase Multifactor Authentication Usage

Objectives

Each year, every department should identify objectives the department hopes to accomplish in the next year. These should align with departmental goals and the MGA strategic plan. In the next section you will be reporting on the objectives you set and whether or not you achieved them in FY22. Later in the document you will report on objectives you hope to accomplish in the coming fiscal year, FY23.

Objective 1

8. Objective 1: What was this department's first objective for this fiscal year? Objectives should be specific, measurable, and achievable within one year.	Cybersecurity will implement a new configuration management system (Intune).
9. Objective 1: Detail specifically how your department measured this objective? (Survey, budget number, number of participants, jobs completed, measurable time and/or effort)	Endpoints enrolled
10. Objective 1: What was your target outcome for this objective? (1.e. 80% participation, 5% enrollment growth, 7% change in engagement)	80%
11. Objective 1: Provide details for your target performance level established (i.e., accreditation requirement, past performance data, peer program review, etc.)	
12. Objective 1: At what level did the department/area achieve on this objective? (This should be a number, i.e., 82%, 6%, 345 attendees, 75% engagement)	0%
13. Objective 1: Did your department meet this objective?	No
14. Objective 1: Improvement Plans and Evidence of changes based on an analysis of the results: What did your department learn from working toward this objective? What changes will you make based on this effort next year?	Scope too broad. Narrowed focus to just IPads and Macs. Will continue to use group policy for configuration management for Windows.

Objective 2

15. Objective 2: What was this department's second objective for this fiscal year? Objectives should be specific, measurable, and achievable within one year.	Cybersecurity will implement a new antivirus software (Microsoft Endpoint Protection)
16. Objective 2: Detail specifically how your department measured this objective? (Survey, budget number, number of participants, jobs completed, measurable time and/or effort)	Windows Endpoints enrolled
17. Objective 2: What was your target outcome for this objective? (1.e. 80% participation, 5% enrollment growth, 7% change in engagement)	) 80% endpoints enrolled.
18. Objective 2: Provide details for your target performance level established (i.e., accreditation requirement, past performance data, peer program review, etc.)	
19. Objective 2: At what level did the department/area achieve on this objective? (This should be a number, i.e., 82%, 6%, 345 attendees, 75% engagement)	98%
20. Objective 2: Did your department meet this objective?	Yes
21. Objective 2: Improvement Plans and Evidence of changes based on an analysis of the results: What did your department learn from working toward this objective? What changes will you make based on this effort next year?	Old antivirus software can be difficult to remove. Will begin installing Microsoft Endpoint Protection on non-Windows computers .

Objective 3

22. Objective 3: What was this department's third objective for this fiscal year? Objectives should be specific, measurable, and achievable within one year.	Cybersecurity will reach 80% completion rate for Fall Cybersecurity Awareness Training.
23. Objective 3: Detail how your department measured this objective? (Survey, budget number, number of participants, jobs completed, measurable time and/or effort)	Number passed.
24. Objective 3: What was your target outcome for this objective? (1.e. 80% participation, 5% enrollment growth, 7% change in engagement)	80% passed.
25. Objective 4: Provide details for your target performance level established (i.e., accreditation requirement, past performance data, peer program review, etc.)	
26. Objective 2: At what level did the department/area achieve on this objective? (This should be a number, i.e., 82%, 6%, 345 attendees, 75% engagement)	86%.
27. Objective 2: Did your department meet this objective?	Yes
28. Objective 2: Improvement Plans and Evidence of changes based on an analysis of the results: What did your department learn from working toward this objective? What changes will you make based on this effort next year?	Getting everyone to complete the training is difficult. Will try to get HR to include supervisor and supervisor email address for import so we can follow up with the employees boss.

Objective 4

29. Objective 4: What was this department's fourth objective for this fiscal year? Objectives should be specific, measurable, and achievable within one year.	Cybersecurity will upgrade 55 older wireless access points in Macon (ADM, TEB, CSS and MATH) and Warner Robins (ASB, OAK, THO) to a more modern standard.
30. Objective 4: Detail how your department measured this objective? (Survey, budget number, number of participants, jobs completed, measurable time and/or effort)	55 Wireless APs replaced.
31. Objective 4: What was your target outcome for this objective? (1.e. 80% participation, 5% enrollment growth, 7% change in engagement)	100%
32. Objective 4: Provide details for your target performance level established (i.e., accreditation requirement, past performance data, peer program review, etc.)	
33. Objective 4: At what level did the department/area achieve on this objective? (This should be a number, i.e., 82%, 6%, 345 attendees, 75% engagement)	100%
34. Objective 4: Did your department meet this objective?	YES
35. Objective 4: Improvement Plans and Evidence of changes based on an analysis of the results: What did your department learn from working toward this objective? What changes will you make based on this effort next year?	Nothing new. Replacing Wireless Access Points is standard operating procedure. No changes.

Future Plans

36. Please identify and detail three to four measurable objectives for the next fiscal year. In listing the objectives, please use the format shown in these examples.1) The Department of X will improve services levels by 5% as measured by our satisfaction survey. 2) The department of X will provide training in ABC for at least 73 MGA faculty and staff.	1) Cybersecurity will pilot a new configuration management system (Intune) for 10 IPADs and 20 Macs. 2) Cybersecurity will implement MFA for 100% faculty and staff using VPN. 3) Cybersecurity will implement Cyberboard requirement to remove local admin access from 80% of Windows endpoints. 4) Cybersecurity will upgrade 6 wireless access controllers to the latest available software.

Open Box for Assessment Comments

37. In this field, please document the overall use of assessment results for continuous improvement of this department area (consider the past, present, and future and specifically address these in your narrative).	Since March 2019 Cybersecurity has seen an increased focus by the University System of Georgia. • The Business Procedures Manual has been updated with new requirements • The IT Handbook has been updated with new requirements • USG Internal Audit has audited for GLBA compliance • USG Internal Audit has audited for endpoint compliance. This has revealed gaps in the current status and desired status of the Cybersecurity department that will be addressed in the future with goals and yearly objectives.
38. Optional Open Text Box for Assessment Comments:	
42. If the COVID-19 pandemic impacted this assessment cycle, please provide specific details below.	Security of VPN endpoints has become more important.

MGA’s Strategic Plan

39. Based on your goals and objectives listed above please indicate their connection with MGA's Strategic Plan	Grow Enrollment with Purpose 1. Expand and

(https://www.mga.edu/about/docs/Strategic_Plan_Overall_DB.pdf) by checking all associated and relevant Imperatives / Strategies from the list below. (Check all the apply)	enrich the face to face student experience Ensure MGA has a good reputation for stewardship of student information and availability of services Grow Enrollment with Purpose 2. Expand and enrich online instruction into new markets Ensure MGA has a good reputation for stewardship of student information and availability of services Own Student Success 3. Develop academic pipelines and expand degrees Own Student Success 4. Expand student engagement and experiential learning Expand Cybersecurity awareness among students in preparation of entering the workforce. Build Shared Culture 5. Attract talent and enhance employee development and recognition Improve Cybersecurity Awareness. Build Shared Culture 6. Sustain financial health through resourceful fiscal management Budget Cybersecurity expenditures wisely and minimized expenses related to Cybersecurity incidents
40. Please indicate which of the following actions you have taken because of the 2021/2022 Assessment Cycle (Note: These actions are documented in reports, memos, emails, meeting minutes, or other directives within the reporting area) (Check all the apply)	Disseminating/Discussing Assessment Results/Feedback to Appropriate External Stakeholders

	Process Changes: Improve, Expand, Refine, Enhance, Discontinue, etc Operational Processes Request for Additional Financial or Human Resources

Other

41. Please indicate (if appropriate) any local, state, or national initiatives (academic or otherwise) that are influential in the operations, or goals, and objectives of your unit. (Complete College Georgia, USG High Impact Practice Initiative, LEAP, USG Momentum Year, Low-Cost No-Cost Books, etc.)	USG Business Procedures Manual implementation Phase 1 and Phase 2 (Privacy) USG Business Procedures Manual implementation Section 3.4.4 (Supplier Contracts) USG Internal audits State Financial Aid Audits USG Cybersecurity Initiatives – Measured with mitigation checklists
43. Mindset Update (Academic Deans ONLY)	