Report- Cybersecurity Risk Assessment of AMC

- **Title Page**- This page contains the name of the group, course ID, section number, the name of team members, and the Aggie Honor Code signed/initialed by each team member.

- **Table of Contents Page**

- **Executive Summary**- No more than a page. Contains a summary of your project goals, your assessment of the cybersecurity risks that AMC faces, and your recommendation to minimize those risks

- **Asset Identification** - A brief explanation of your task in this phase of the project and the list of assets identified by your team. This information is available on pages 5 & 6. IT assets at Tier 3 (according to NIST classification) include all the workstations, servers, firewall PC, router, and switches. All IT assets with the same OS should be counted as one asset. For example, all PCs running on Windpws 7 should be listed only once in the IT asse Inventory. [NOTE: you will lose points if you do not provide a rationale for including an asset in this list].

- **Vulnerabilities-** Identify technical and other vulnerabilities for each asset. This information is available on page 7, and also in the data from survey and interviews of AMC employees. If you are confused about whether to consider something as a vulnerability, ask yourself the questions- *How can a threat agent (e.g., an AMC employee and/or outside hacker)* take advantage of this "vulnerability", i.e., exploit it to compromise the confidentiality. Integrity, and/or availability of the asset in which this vulnerability is present? If you are unable to answer this question, then ignore this "vulnerability". Example-

Asset Name/ID/Code	Brief description	Vulnerability	Evidence
W7	Workstations running Windows 7 OS	CVE-2015-6131	Pen testing report
		Auto logout after some inactivity is disabled	Table 9, Page 14, "Staff Areas of Concern".

NOTE: If you need more space to provide the details of a vulnerability, then provide these details in an appendix. If you use the NIST guidelines for risk assessment, then this step in covered in TASK 3 (Page 2 of the case study).

- **Threat Identification**- A brief explanation of your task in this phase of the project. Provide (in table format) the threat statements for each asset and vulnerability in that asset. Based on your project guidelines, you should have at least 4 threat statements for each asset, and these statements should include at least two technical vulnerabilities (with CVE IDs) and two non-technical vulnerabilities (due to gaps in administrative and physical controls). Refer to the appropriate appendix for explanation of the vulnerabilities. Example-

Asset Name/ID/Code	Vulnerability	Threat	Threat Agent/Source	Exploit
W7	CVE-2015-6131	Code execution from remote location	Outside hackers	crafted .mcl file (Source: https://nvd.nist.gov/vuln/detail/CVE-2015-6131)
	Auto logout after some inactivity is disabled	See patient data on the workstation screen	AMC Employees not authorized to access patient data	Observe the unlocked workstation

NOTE: If you need more space to provide the details of a threat and how it happens, then provide these details in an appendix. If you use the NIST guidelines for risk assessment, then this step in covered in TASK 1 and 2 (Page 2 of the case study).

- **Likelihood of Threat**- A brief explanation of your task in this phase of the project. Provide the scale used to measure the likelihood of a threat happening. See the presentation slides for various options to define the likelihood measurement scale. Example-

Likelihood Measurement Scale

Definitely	Likely	Unlikely
The threat will happen	The threat may happen	The threat won't happen

Asset Name/ID /Code	Vulnerability	Threat	Threat Agent/ Source	Exploit	Likelihood

W7	CVE-2015-6131	Code execution from remote location	Outside hackers	crafted .mcl file (Source: https://nvd.nist.gov/vuln/detail/CVE-2015-6131)	Definitely
	Auto logout after some inactivity is disabled	See patient data on the workstation screen	AMC Employees not authorized to access patient data	Observe the unlocked workstation	Likely

NOTE: If you need more space to provide the details of why you give a certain likelihood score to a threat, then provide these details in an appendix. If you use the NIST guidelines for risk assessment, then this step in covered in TASK 4 (Page 3 of the case study).

- **Impact of Threat**- A brief explanation of your task in this phase of the project. Provide the scale used to measure the impact if a threat happens. See the presentation slides for various options to define the likelihood measurement scale. Example-

Impact Measurement Scale

Critical	Moderate	No Impact
Confidentiality, Integrity, and/or Availability of the target asset are completely compromised	Confidentiality, Integrity, and/or Availability of the target asset are partially compromised	Confidentiality, Integrity, and/or Availability of the target asset are not compromised

Asset Name /ID /Code	Vulnerability	Threat	Threat Agent/ Source	Exploit	Impact
W7	CVE-2015-6131	Code execution from remote location	Outside hackers	crafted .mcl file (Source: https://nvd.nist.gov/vuln/detail/CVE-2015-6131)	Critical (https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2015-6131&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C)&version=2.0&source=NIST)
	Auto logout after some inactivity is disabled	See patient data on the workstation screen	AMC Employees not authorized to access patient data	Observe the unlocked workstation	Moderate

NOTE: If you need more space to provide the details of why you give a certain impact score to a threat, then provide these details in an appendix. If you use the NIST guidelines for risk assessment, then this step in covered in TASK 5 (Page 3 of the case study).

- **Risk to IT Assets**- A brief explanation of your task in this phase of the project. Provide the Risk Matrix used to estimate the risk to an asset from each vulnerability-threat pair. Example-

RISK MATRIX				
	IMPACT			
LIKELIHOOD		CRITICAL	MODERATE	NO IMPACT
	DEFINITELY	HIGH	MEDIUM-HIGH	LOW
	LIKELY	MEDIUM-HIGH	MEDIUM	LOW
	UNLIKELY	LOW	LOW	LOW

RISK ESTIMATES						
Asset Name	Vulnerability	Threat	Threat Agent/ Source	Likelihood	Impact	Risk

/ID /Code						
W7	CVE-2015-6131	Code execution from remote location	Outside hackers	Definitely	Critical	HIGH
	Auto logout after some inactivity is disabled	See patient data on the workstation screen	AMC Employees not authorized to access patient data	Likely	Moderate	MEDIUM

NOTE: If you use the NIST guidelines for risk assessment, then this step in covered in TASK 6 (Page 3 of the case study).

- **Cyber Security Risk Management Strategy**- Provide cybersecurity risk mitigation strategy for each threat statement.
- **References**
- **Glossary-** Provide a brief explanation of terms and abbreviations to explain them to a reader who is not an expert in information systems and/or cybersecurity

Additional Suggestions

1. Number and label each table and figure and provide cross references to improve the readability of the report.
2. Number the pages.
3. Proofread for grammatical and/or spelling mistakes.
4. Format the report to improve its readability.