## Learning Outcome of the Assignment

1. Propose the security techniques that might form part of a defensive strategy. (A5, PLO5)

2. Compare various techniques used in the defense of computer systems against malicious software and software-based attacks. (A4, PLO9)

## Instructions:

No marks will be awarded for the entire assignment if any part of it is found to be copied directly from printed materials or from another student. All submissions should be made on or before the due date. Any late submissions after the deadline will not be entertained. **Zero (0)** mark will be awarded for late submission, unless extenuating circumstances are upheld.

## Questions:

You are required to conduct research individually.

The Internet of Things (IoT) has given rise to numerous new technological solutions that are utilised by numerous industries. The Internet of Medical Things (IoMT) is essential for improving the accuracy, dependability, and productivity of electronic equipment in the healthcare sector. Typically, the doctors advise their patients to "Listen to your body and take heed of what it is saying to you." The IoMT devices as part of new technologies will now listen for us and evaluate the signals to help choose the best course of action. The Internet of Medical Things (IoMT) is a network of connected medical equipment and software. These medical gadgets' Wi-Fi connections allow them to connect to cloud services like Amazon Web Services, where the acquired data can be stored and analyzed.

As IoMT is becoming popular nowadays, you are required to do research on this area. Your research should focus on ONE IoMT device or system only. In your research, you should include the followings:

1. Discuss the vulnerabilities of current system or device.
2. Identify and discuss the possible type of exploits that might occur to the IoMT devices or system and their impacts.
3. Perform risk assessment of the device or application platform based on the type of exploitation discussed above and support your statement with Mitre attack framework.
4. Discuss organizational security, operational security and methods of defense that can be implemented to prevent from the example of attack mentioned above. Provide business continuity and disaster recovery plan.
5. You may propose the improvement of existing security of IoMT devices/system with either Conceptual model or framework or simulation.

## Assesment

This assignment will contribute 30% towards the incoure marks,as mentioned on the Student Assesment &Information sheet

This assignment will be evaluated based on the following criteria.

## Assessment Criteria (Marks Breakdown)

| Marking Criteria | Weighting | Marks |
|---|---|---|
| **Section A** | 100 | |
| Vulnerabilities and possible attacks. | 30 | |
| Risk Assessment, Business Continuity and Disaster Recovery | 30 | |
| Organizational Security, Awareness and Information Sharing | 20 | |
| Conceptual Model/framework | 20 | |
| Total | 100 | |

## Guidelines for the Report:

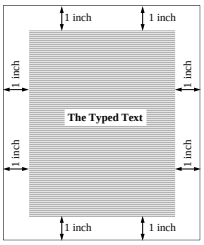
Document the results of your work in a **professional and systematic** manner, in the form of a **computerized report**. **One (1)** softcopy of your documentation is to be submitted.

Your completed documentation should meet the following requirements:

1. Table of contents for every detailed chapter/section.
2. Abstract
3. Introduction
4. Chapters / sections
5. Conclusion
6. Appendices
7. References

## Submission requirements

1. Your report must be typed using Microsoft Word with Times New Roman font. You need use to include a word count at the end of the report (excluding title, source code of program & contents pages) Report should be in 1.5 spaces.
2. The report should have a one (1") margin all around the page as illustrated below:




3. Every report must have a *front cover*. The front cover should have the following details:-
   a) Name
   b) Intake code.
   c) Subject.
   d) Project Title.
   e) Date Assigned (the date the report was handed out).
   f) Date Completed (the date the report is due to be handed in).
4. **All** information, figures and diagrams obtained from external sources **must** be referenced using the APA referencing system accordingly.

**Marking Scheme Rubrics**

| Criteria | Fail | Pass | Credit | Distinction |
|---|---|---|---|---|
| **Vulnerabilities and possible attacks. (30)** | Poor research and investigation of the cyber vulnerabilities. Poor evaluation of the requirement. | Well research and investigation is done. Good evaluation of the requirements with proper reasoning with proper planning and management. | Well analysis and investigation of the problem. Acceptable evaluation of the requirements with proper reasoning. Acceptable planning and management with detail research | Very well analysis and investigation of the problem. Outstanding evaluation of the requirements with proper reasoning. Outstanding planning and management with detail research |
| | Fail | Pass | Credit | Distinction |
| **Risk Assessment, Business Continuity and Disaster Recovery (30)** | Poor research and investigation of the business continuity and disaster recovery plan | Acceptable research and investigation are done. Acceptable business continuity and disaster recovery plan with proper reasoning, planning and management strategy. | Good analysis and investigation are done. Good business continuity and disaster recovery plan with proper reasoning, planning and management strategy. | Very well analysis and investigation are done. Outstanding business continuity and disaster recovery plan with proper reasoning, planning and management strategy with detail research |
| | Fail | Pass | Credit | Distinction |
| **Organizational Security, Awareness and Information Sharing (20)** | Poor and lack of research and investigation of the organizational security, awareness, and information sharing | Acceptable research and investigation are done. Acceptable organizational security, awareness and information sharing discussed | Good analysis and investigation are done. Good organizational security, awareness, and information sharing discussed | Very well analysis and investigation are done. Outstanding organizational security, awareness and information sharing with detail research |
| | Fail | Pass | Credit | Distinction |
| **Conceptual Model/framework (20)** | No conceptual diagram provided or | Conceptual diagram/framework provided but | Conceptual diagram/framework provided | Outstanding conceptual diagram/framew |

| | | | | |
|---|---|---|---|---|
| | provided with wrong concept in terms of cyber security implementation | explanation is not clear | with clear and detail explanation | ork provided with excellent idea and innovation and detail explanation. |