Infosec of AI Systems – Team Matrix
Multiple Choice Questions

Team Members: Prachi Sinha, Pavan Chandra Sanda, Bhavana Yetinthala, Sai Vineeth Grandhi, Tharun Reddy Sabbasani
Section: S4 (9:30 AM to 10:50 AM)

1. **What is the flow of steps for maintaining an AI model Architecture?**
   1 Model Learning
   2 Requirements
   3 Model Tuning
   4 Data Management
   5 Model Maintenance
   6 Model Deployment

   a) 1-2-3-4-5-6
   b) 2-4-1-3-6-5
   c) 3-6-1-2-4-5
   d) 6-5-4-3-2-1

   Answer: b) 2-4-1-3-6-5

2. **What are the types of risks associated with AI?**
   a) Data Related Risks
   b) Privacy Risks
   c) Testing and Trust
   d) All the above

   Answer: d) All the above

3. **What are the types of attacks associated with AI?**
   a) Evasion Attack
   b) Poisoning Attack
   c) Backdoor Attack
   d) Stealing Attack
   e) All the above

   Answer: e) All the above

4. **What is the name of defensive technology associated with data collection in stealing attack?**
   a) Adversarial Samples
   b) Data Filtering
   c) Regression Analysis
   d) Differential Privacy

   Answer: d) Differential Privacy

5. **What is the name of defensive technology associated with model training in backdoor attack?**
   a) Network Distillation

b) Ensemble Analysis
c) Model Pruning
d) Model Watermarking

Answer: c) Model Pruning

6. **What is the name of defensive technology associated with model inference in evasion attack?**
   a) Adversarial Detection
   b) Input Reconstruction
   c) DNN Model Verification
   d) All the above

   Answer: d) All the above