

Agentic AI Security Guidelines

Enable logging for monitoring and auditing

Application of least privilege rule

Limiting read write scope of agent

Time limited credential setup

Stress testing of potential threat modelling scenarios

Dependencies mapping

Incident Planning In Case of Any Cyber Attack/Disaster

Apply rigorous governance policies on end to end agentic AI architecture

Applying authentication monitoring and auditing best practices on the users of Agentic AI