**Student Name:** **Weight: 5%**

**Student ID:** **Marks: /**

# Instructions

A ransomware attack has been reported by a user at your company. The data residing on the user’s computer has been encrypted and a notice page is displayed on the screen demanding bitcoin payment. Unfortunately, due to budget constraints your security team has not yet developed an incident response plan.

1. Given what you know about the incident response phases, devise a simple incident response plan to address this ransomware attack.
2. Briefly describe what actions and measures are required to address each phase.
3. What security tools would you use to handle the incident?

# Incident Response Phases

1. Triage phase: Determine the level of the incident and eliminate false-positives.
2. Investigative phase: Analyze the incident for appropriate reactions and recovery procedures.
3. Containment phase: Contain the incident to limit the damage and impact.
4. Analysis and tracking phase: Analyze what has occurred and what damage was done. Track the incident back to determine the initial entry point and root cause.
5. Recovery phase: Put a solution in place to address the root cause and to recover from the incident and the damage caused.