**Scenario:**

An oil company’s senior management has reason to suspect that John Smith, one of the company’s mechanical engineers allegedly took information that was clearly identified as proprietary. The company’s legal office has requested digital evidence regarding the potential violation of company policy, which prohibits the sharing of proprietary information without prior approval. The employee was not authorized to access proprietary information. All employees sign nondisclosure agreements (NDAs) and acceptable use policies (AUPs). Senior management and the legal office have approved this request.

**Investigative Plan:**

  This investigative plan will provide a clear outline of actions to be taken during the investigation.

1. Discuss the strategy that your team will use to both maximize the collection of evidence and minimize the impact on the organization.
   1. A briefing prior to engagement to set expectations of data collection. Ensuring the team has a clear understanding of what they are looking for during the investigation.
   2. This should provide as much detail surrounding the scope of evidence as possible. This will speed up collection times.
2. Describe the tools and techniques your team will use in evidence gathering, preparation, and analysis.
   1. Memory dump of the system with Dumpit
   2. The team will perform a memory dump using a tool named Dumpit. This will capture volatile information ensuring a full forensic scan is performed.
   3. The tool to be used during the investigation will be Autopsy.
   4. The team will identify beforehand any systems the suspect has access to.
   5. The team will immediately take those machines into custody and ensure they are isolated and offline. This aids in minimizing impact to the organization and ensures the remaining resources are left to work with.
3. Describe how your team will collect and preserve required evidence, using standardized and accepted procedures.
   1. The team will isolate the machines in question, removing them from the network. The team will ensure the chain of custody is followed.
   2. Here Autopsy will be used to collect information from the system ensuring the team collects any deleted files, captures the partitions, and any data files associated.
4. Describe how your team will examine the seized evidence to determine which items are related to the suspected violation of company policy.
   1. Upon review of the information the team will begin to determine what information may be flagged as confidential. This can be done through a series of key word searches, manual review of documents found.
5. Discuss an approach that your team will use to draw conclusions based on the digital evidence that supports the claim of a policy violation.
   1. The team will work with the facts. If a document is marked as confidential it will be flagged and brough to the appropriate teams, i.e. HR, Legal. The team’s role is to capture intelligence or information building the “story” it is up to the HR and Legal teams to determine action.
   2. The team will include any supporting evidence that would indicate a motive.
6. Discuss how the case details and conclusions should be presented to senior management.
   1. A high-level summary of the detailed information will be provided to the senior management teams. This summary should not be “technical” but should detail the facts found in common terms.