C840 TASK 1

A1: Discuss the strategy that your team will use to both maximize the collection of evidence and minimize the impact on the organization.

A meeting will be held between the senior management, legal office, and investigation team prior to beginning the investigation regarding this case. The investigation team will be informed of the details of the case and that there is a legal hold placed on evidence that's been approved by the Legal Office and Senior Management. Senior management suspects that their mechanical engineer, John Smith, had unauthorized access and shared proprietary information, breaching the company's AUP and NDA. The goal of the investigation team is to identify, preserve, and verify relevant digital evidence from John Smith's office and computer. The investigation team will first secure the perimeter of John Smith's office with caution tape to block unauthorized personnel from entering. Securing the area ensures that the evidence remains preserved and intact, ensuring integrity.

A2: Tools and Techniques- Describe the tools and techniques your team will use in evidence gathering, preparation, and analysis.

The tools and techniques for gathering evidence will be using FTK imager and a write blocker. FTK imager is a forensic imaging tool that allows a bit-by-bit level copy of the contents of John Smith's hard drive, ensuring the data copied is in its original state. The write blocker must be used to ensure that no modifications have been made to John Smith's original hard drive. Before creating a disk image, a cryptographic hash value (MD5 or SHA1) must be generated on the contents of John Smith's original hard drive. This provides a baseline hash value that can be used to verify the data integrity. Then, use the forensic imaging tool, FTK imager, to create the disk image, ensuring the copied data matches the original hard drive data. After the disk image is created, the same cryptographic hash function (MD5) is performed to generate the hash value to ensure it matches the contents of the original hard drive. The next step is to use the FTK imager's memory acquisition tool to prioritize preserving sensitive data based on the order of volatility to ensure data will not be lost if the power goes down. The order of the most volatile data to least volatile is CPU, RAM, and hard disk. The autopsy tool or FTK imager can be used to examine the disk image created from the hard drive.

A3: Collection and Preservation of Evidence- Describe how your team will collect and preserve required evidence, using standardized and accepted procedures.

The standardized and accepted procedures being used by the investigation team will be chain of custody outlined by NIST “A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.” This process begins with evidence collection using a write blocker to prevent data from being modified, then completing a chain of custody form. The chain of custody form contains the evidence's unique identifier, the Investigation Team member's name, and the evidence condition. The next step is preserving the evidence by sealing the evidence in a tamper seal package in a secure facility to prevent unauthorized access. The next step is transferring evidence; each time the evidence is transferred to a different individual or location, the evidence’s condition is verified, and the record of transfer details is documented in the chain of custody of logs. The last step is evidence analysis, which checks the hash value of the evidence to ensure the data hasn’t been modified.

A4: Examination of Evidence- Describe how your team will examine the seized evidence to determine which items are related to the suspected violation of company policy.

The investigation team will use FTK imager and File carving techniques to analyze the file system from the disk image created from John Smith's hard drive. It is starting with searching for unauthorized file access logs and file transfers, including preserving the time stamps and file logs that identify breaches of company policy. The procedure will begin by using search filters and keywords related to the company's proprietary information, using the Company's AUP and NDA documentation as references. This will validate and verify any violations made to company policy.

A5: Approach to Drawing Conclusions- Discuss an approach that your team will use to draw conclusions based on the digital evidence that supports the claim of a policy violation.

The approach the investigation team will use to draw conclusions based on digital evidence is to ensure the digital evidence collected wasn't modified and the investigation followed company policy procedures and guidelines. The team will review and summarize the collected evidence containing the proprietary information found on John Smith's hard drive that breached the AUP and NDA for the company. This includes the time stamps, logs, and files found containing the digital evidence needed to support Senior Management and the Legal Office.

A6: Presentation of Details and Conclusions- Discuss how the case details and conclusions should be presented to senior management.

The investigation team will format and prepare a concise report for Senior Management and the Legal Office. This report will avoid technical jargon, providing a summary highlighting the key findings, investigation process, and analysis performed on the evidence that led to the policy violations by John Smith. A visual aid PowerPoint that includes charts and graphs will be used for the presentation, along with a copy of the report for Senior Management. By following these guidelines, the Investigation Team followed best practices for forensic investigation by following the chain of custody, preserving the integrity of data throughout its lifecycle.

References:

Chain Of Custody. National Institute of Standards and Technology (NIST) (n.d)
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-72.pdf