**INVESTIGATIVE PLAN OF ACTION**

The team members will collect data from a targeted system from a company computer that was accessed by John Smith while following best practices to ensure the integrity of the evidence. It is very important to follow a structured and methodical approach. We can start by collecting volatile data from the CPU, cache, and RAM before that can quickly disappear. Documenting and taking photographs of the screen and devices before removing anything during the evidence collection process. We will be using trusted tools when collecting data to maintain the integrity of the evidence. Following the chain of custody of all the evidence collected will ensure it is admissible in court. If the computer is off, it will stay that way to avoid altering the data. If the computer is on then we will be able to conduct and collect live data from the running system and examine the system processes that are running, login users, and network connections. We will be securing the storage that will be collected as evidence and those will be in a secure location to avoid tampering or loss of data. With our regular training, the team will be able to take the proper procedures while collecting evidence. There will be a minimal impact on the organization’s network when investigating to avoid business disruption. This will also not affect financial or business operations.

The forensic tool that the team will use and has experience with is EnCase which will be used for imaging the hard drive and live search, capturing network traffic, and reviewing system logs. When doing live searches on John Smith’s computer the procedures must be done correctly as some information can be on volatile memory which temporarily stores data and can be lost. Once we have the image of the computer hard drive, we will use our tools on the copy and not the original hard drive for the investigation. FTK tool will be utilizing features such as cracking passwords, analyzing emails, file decryption, and data carving. It is always best to use more than one tool while doing digital investigations as the courts accept the software’s capabilities. Also, while searching, the integrity of the evidence must be done correctly such as hashing techniques to compare hash values of the original evidence collected.

The team will collect and preserve the evidence using standardized and accepted procedures to ensure the integrity of the evidence in a legal proceeding. This can be done by securing the scene to prevent contamination or loss of evidence. By documenting everything such as photographs and detailed notes evidence at the scene before moving the computer or attached devices. Following the chain of custody will help maintain the evidence collected including when, where, and how that was collected along with the transfer of custody. The team will be using labels, anti-static bags, and containers to prevent temperature damage or contamination of the evidence. If digital evidence is discovered, we will be using write-blockers to prevent the alteration of data. Our team will be following the standard procedures provided by the National Institute of Standards and Technology (NIST) which is credible throughout the investigation.

As a team, we will examine the seized evidence and determine the items related to the suspected violation of company policies. The oil company did make all the employees sign nondisclosure agreements (NDAs) and acceptable use policies (AUPs). This would cover how the employees can use their computers for work and understanding the confidentiality of client information shared. Reviewing the company’s policy will help the team determine the suspected violation to see what evidence will be relevant. We can then proceed and categorize the digital evidence collected which can be emails, files, and network logs to see if data was transferred, or any other devices that were used on the computer to link the policy breach. This will all be documented for legal proceedings.

Based on the digital evidence that supports the claim of policy violation our team has helped conclude by following the proper procedures. We have been able to search and discover files along with system access logs that violated company policies. The team has been able to examine the data’s date and time that was accessed by John Smith and compare where company policy was violated. When John Smith signed the nondisclosure agreements (NDAs) and acceptable use policies (AUPs) agreed to follow company policies. Our team has determined there was unauthorized access from John Smite of the proprietary data.

After the team has completed the digital forensics and followed the standardized procedures, we are ready to present to senior management our completion of work. Documentation will be provided to senior management explaining our findings and detailed information on where the policy was violated by John Smith. Below is the digital forensics report performed by our team.

Title: John Smith Violation of Company Policies on Proprietary Data

Introduction:

* Purpose: John Smith is the company’s mechanical engineer who is accused of accessing data that is identified as proprietary and belongs to the oil company.
* Objective: John Smith took information that was identified as proprietary. The sharing of proprietary information without prior approval is a violation of company policy.

Background:

* All employers at the oil company have signed a nondisclosure agreement (NDAs) and acceptable use policies (AUPs) which makes them acknowledge that access to proprietary information will need to be authorized.
* Timeline of events have been documented with date and times.

Tools Used: EnCase and FTK.

Steps during the investigation:

1. The team started photographing the computer at the scene.
2. If the computer is off, we will leave it as is until we can get this back to the forensics lab. If the computer is on, then will take a photograph of the screen.
3. As we collect live data, we started looking at the RAM image to collect live data as the user's login logs, network connection state, or unusual processes that are running on the computer.
4. We then analyze the computer hard drive to see if that has encryption so that we can create an image with one of our forensics tools and keep the original data collected intact.
5. Since the computer was on, we could just unplug the power and not shut down the computer properly which would help our investigation.
6. Once that has been done, we will create a diagram and label all the cords before removing them from their current location.
7. At this point, we can document the computer model numbers and serial numbers and any devices that were connected.
8. The team has disconnected all the cords and devices after ensuring all of that has been properly documented.
9. Next, we package all the components collected using anti-static evidence bags and containers. While doing the seizure of the equipment we kept that away from magnets, radio transmitters, or any other potentially damaging elements.
10. Lastly, we have documented all the steps used in the seizure.

Conclusion: We have identified John Smith access company proprietary information on different dates and times.

Recommendations: Conduct regular security audits and enhance employee training.