**A1**

The investigation team will meet with the relevant management parties of the oil company and the legal department to ensure everyone is on the same page about the investigation before doing anything else. Each party will assist in gathering the necessary information to ensure that the investigation process moves along efficiently. The legal department will explain the policies they suspect have been violated by John Smith while providing copies of the AUP and NDAs signed by John Smith and obtaining the necessary permissions to collect digital evidence. The first thing that should be done after the initial meeting to discuss the situation is for the investigators to create a baseline of John Smith and his job role/expected access rights. This will help in conducting an anomaly analysis to see whether anything has changed, and if so, then what has changed and why.

The investigation team will decide on the scope of the investigation and begin taking photos and documenting everything at the workspace(s) in question, making sure to leave everything in its original state. After the opening documentation has been completed, the investigators will begin recording the volatile data from the workstation(s) used by John Smith using the Volatility tool. The hard drive will then be copied exactly how it is using FTK Imager. This will create a bit-by-bit copy of the hard drive, ensuring that it is as close as possible to the original. Investigators will then begin analyzing the network traffic using Wireshark to check for any questionable packets leaving/coming into the network. Performing these actions quickly will ensure business continuity while adhering to best forensic practices. The workstation(s) will be fully documented within the chain of custody and remain untouched and secure for the remainder of the investigation.

**A2**

Investigators will use various tools to collect and analyze data and evidence, such as:

* Camera - Investigators will use the camera to document the original workspace(s) for photographic evidence.
* EnCase – Used for imaging hard drive(s).
* Volatility – This will capture data from volatile memory sources from the workstation(s).
* FTK Imager – Creates bit-by-bit copy of the workstation(s) in question so that the original evidence remains untampered with.
* Autopsy – A tool for analyzing images of the workstation(s), helping investigators uncover the contents of the drive(s), including data that has been erased.
* Wireshark – Used to capture/analyze network traffic to see if any suspicious packets/communications are being sent over the network.
* Log analyzer – Investigators will use an analyzer to review system logs and other relevant logs to track questionable behavior on the workstation(s)

**A3**

The investigation team will ensure they have the legal authority to search through the device(s), which can be obtained through consent or a search warrant (*Quality Standards for Digital Forensics* 2019). Maintaining a strict chain of custody to ensure the integrity of the evidence is of utmost importance. The investigation team will take photos of everything before touching or accessing any system storing evidence. Using various forensic tools, they will use appropriate and accepted procedures to obtain evidence while leaving the original system how it was found by creating a full copy of the workstation(s) image. Then, they will review the relevant system logs to determine when unauthorized access occurred. Using Wireshark, the team can see what traffic was passing over the network during the unauthorized access. They will also ensure the integrity of physical storage mediums using proper handling/transporting techniques, such as static-resistant bags. The team will thoroughly document everything seen/done/found and by whom.

**A4**

The information gathered at the initial meeting will be used to determine what evidence is relevant to the investigation, such as the company policies, AUP, and NDAs provided by the legal department. This information can be used to find keywords and determine if any proprietary information can be found in the evidence obtained from John Smith's workstation(s). The disk image and copies of the volatile memory will be searched for any content that John Smith should not have access to. The logs will be analyzed to determine if any connections were made to outside networks and be investigated further to discover any proprietary information.

**A5**

After understanding the situation, using the information from the AUP, NDAs, company policy, and evidence collected, the investigation team will compare the evidence found to determine what employees are authorized to access and what information should be considered proprietary. After the evidence is analyzed and compared to the documentation provided, the investigators should be able to conclude whether or not John Smith is guilty of the allegations that are against him.

**A6**

The case details and conclusions should be presented to senior management in a clear and concise manner, such as through PowerPoint presentation. It should include essential information, such as the scope of the investigation, what procedures were followed during the collection of evidence, as well as throughout the investigation, and also how it corresponds with the company's AUP, NDAs, and policies. I would include any photos taken during the investigation, charts, and graphs to give a visual understanding of the case. I will also ensure that minimal technical language is used, as that can seem confusing to people who may not be familiar with the investigative process. These are all things that can be utilized to ensure the information is easily understood and everything is clear.

References

Quality Standards for Digital Forensics. (2019, June 18). https://www.ignet.gov/sites/default/files/files/Quality\_Standards\_for\_Digital\_Forensics\_2019.pdf