(You’re Name Here)

**Executive Summary**

* Three paragraphs
* Provides the readers direction regarding conducting an investigation involving any type of incident that may require assistance from a forensic investigator.
* The goal of the forensic plan is to provide guidance to the readers when a forensic investigation is requested and will allow the reader to understand the necessary steps that are required to be taken in order to perform a proper investigation.
* The Forensic Plan does disclose first response roles and responsibilities. The use of this document will come into play once an incident has been verified and it has been determined that a forensic investigation is needed to take place.
* The forensic plan document is in a sense a checklist of steps that the e-discovery investigation is required to go through and a template for recording the steps taking during the computer forensics investigation.
* The forensic plan acknowledges that each investigation is unique and each investigation can have various contributing factors, which can or cannot not be identified during the pre-data collection phase of the investigation.
* Each investigation has required components and these components create the general framework and investigation checklist. These components are the required phases each forensic investigator must properly go through: Data Collection, Examination, Analysis, Reporting, and Recommendation is not required but can be provided if desired or requested.
* This document illustrates the simple elements of a Forensic Plan from the first initial phase, Data Collection, to the final phase, Reporting. As the investigation takes place and goes through the required steps, checklist items will be accomplished and the results of the phases and overall investigation will be documented in the plan.
* During the investigation, the forensic professional may discover other information relating to other activities outside the scope that may need to be documented with additional research. It is their responsibility to decided what evidence is essential to their particular investigation.

**Terminology**

1. Breach: Data is in the hands of an unauthorized user.
2. Chain of Custody: The chronological documentation or, showing the seizure, custody, control transfer, analysis, and disposition of physical or electronic evidence.
3. Digital Forensics: A scientific method of gathering data and examining for the purpose of presenting in court.
4. Electronic Discovery (E-Discovery): The process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.
5. Electronically Stored Information (ESI): Any type of information that is created, used, and stored in digital forms, and required a computer or other devices for access.
6. Event:. Can be anything. One believes something has occurred, but additional effort is required in order to validate.
7. Incident: Something has occurred.
8. Internal Threat: Comes from sources that are within an organization’s network.
9. Legal Hold: A process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated.
10. Live Acquisition: Maintaining current state of machine.
11. National Security Letter (NSL): An administrative subpoena issued by the United States government to gather information for national security purposes.

**Data Collection**

1. **System/ Technology**
   1. Limit scope of systems
   2. No specific technology the investigators are limited to
      1. Briefly mention emails, phone logs, text messages, hard drives
   3. Support HR system (payroll), cyber systems
2. **Process/ Procedure**
   1. Responsibility of the IT person to know where the evidence is and how to find it.
   2. Need to address data size
   3. Need to be proactive and not reactive
   4. Be familiar with the lingo of the industry
   5. Involve the entire litigation team and client involved for data and review
   6. No straight process
   7. Track and document everything
   8. Do everything possible to ensure no data is modified
   9. The individual conducting the investigation must be competent
   10. Keep a clear log of exactly what the investigator does
   11. The person in charge has overall responsibility for ensuring that the law and principles are adhere to.
3. **Interviews/ Investigations**
   1. A chief info sec office who delegates all work to director of security.
   2. Director conducts the investigations and interviews
4. **Chain of Custody**
   1. Collecting materials (data) and preserve
   2. Keep track who has possession/custody of evidence and where something went wrong
   3. Evidence stack

**Examination**

* Assessing and picking out relevant pieces for the investigation

**Analysis**

* Breakdown of the data and drawing conclusions from it
* Determining who did what or is doing what?, when was it done?, what changed?, why are they changing something?

**Reporting**

* Preparing and presenting the results conducted from the analysis
* Non-bias
* Included in the report is the process (everything stated above)
* Report can go to the requester of the investigation/ presented in court

**Recommendation**

* Investigator provides his/her recommendation from their point of view
* Not required