(You’re Name Here)

**Forensics Plan**

**(Draft)**

**Executive Summary**

This forensics plan includes the requirements and procedures for collecting digital evidence in response to incidents that would determine affected resources, extent of damage, involved parties, responsible personnel, data collection and preservation activities, potential evidence examination, analysis and report of findings.

During the investigation process, an incident will be assessed with its situation, impact, case specifics and characteristics, which will help to define best approach to identify, preserve and collect evidence. Justification will be made on what systems to take down and how data can be acquired without affecting volatile data.

Further, timeline analysis and sorting through large data sets will be performed in order to find useful evidence using various modern tools that would reduce amount of data to be analyzed.

**Terminology**

Litigation Hold - Written directive advising custodian of ESI preservation requirements

ESI - Electronically Stored Information

Legal Letter - A letter from an attorney at law advising on legal case or demands

Digital Evidence - An electronic data that can be presented at a court of law as evidence

Chain of Custody - Chronological documentation or paper trail

Incident - An individual occurrence of an event

Investigation - A process of identifying evidence admissible in the court of law

SOP - Standard Operating Procedure

**Data Collection**

In response to an incident, an effective forensics investigator should require a response team to collect data with respect to identification, recording, reproducing, copying and storing data in timely manner. An event specific information must be obtained from as many sources as possible to preserve all pieces of evidence while conquering challenges of volatile data, limited logging, etc.

* **Systems/Technology**

Diversity of technologies pose significant challenges, so it is necessary to identify source any number, type and location of potential evidence based on capabilities of existing technologies such as understanding logging capabilities, synchronization of data across various systems on-premises and in the cloud, backups, archival, retention and automated deletion.

* **Process/Procedure**

SOPs and guidelines should be developed for appropriate preservation and handling of digital evidence including addressing basic steps for conducting investigation, processing, handling and preserving evidence. All available and related information should be collected as it relates to potential evidence

* **Interviews/Investigations**

It is required to identify who is doing investigation and who is involved in the interview process. Identify legal authority for examination request and consult with case investigator to make sure it is understood what can be discovered, what may not be discovered, what items will be taken for forensics data collection. Also, discover all opportunities for additional data collection from external partners and resources. Consider relevance of items to be searched.

* **Chain of Custody**

Detailed paper trail and full documentation in chronological order must be performed and preserved while following full consistency of the entire process. Document should follow process requirements and be completed on the appropriate forms as approved by appropriate departments.

**Examination**

Different types of cases may require various methods of ESI examination; therefore, persons conducting an examination should be well trained to be aware of various methodologies and techniques. Moreover, persons examining data should be delegated with appropriate examination responsibilities and activities while having a presence of a single point of contact of the entire process. Also, examination process should include specific list of who is doing examination. An examination should be conducted on acquired data with acceptable forensics procedures and on non-original data; that is, use preserved data for examination purposes.

**Analysis**

Interpretation of recovered data and identification of logical correlation that would be useful and in readable format with all details such as how data was acquired, from which media, and the content and purpose of the found evidence. The extracted and identified evidence should be valuable to the case, so certain methods that may be used include timeframe for events occurrence and correlation, reviewing time and date stamps, who and when modified data, reviewing hidden and compressed files, applications and files structure.

**Reporting**

The examiner is responsible for providing a complete and accurate report of findings and results of the analysis as it relates to digital evidence followed by thorough documentation throughout the investigation process with all performed steps. Report should be prepared for targeted audience with all notes, reference to materials, litigation holds, legal letters, signatures, erased and recovered files, and other related documentations.

**Recommendation**

Any outcome that is not part of the report should be reported as recommendations. An investigation that revealed a weakness in technology or process requires a change in organizations own process and procedure that would significantly improve future forensics cases, such as recommendation for better retention policy for backup and emails that might improve future investigation cases.