(You’re Name Here)

Forensic Plan Outline

Executive Summary

* This plan will document general procedures in case of a criminal incident involving corporate IT resources. The primary objective will be to instigate a set of procedures that will effectively:

1. Determine the nature of the crime
2. Determine the number and location of affected resources
3. Determine the extent of damage to corporate resources, customers and partners
4. Isolate affected resources from the production network
5. Identify and isolate affected users from the network
6. Document all process and evidence for law enforcement officials

Terminology

* Terms related to the investigation of digital devices and media
  1. Acquisition
  2. Digital media
  3. E-discovery
  4. Breach notification
  5. Internal Threat
  6. External Threat
  7. Live analysis

Data Collection

* An outline of the processes and procedures that should be followed when collecting data to determine if an incident has taken place

System/Technology

* Systems and technology that will be used during forensic activity i.e. central file viewer, write blocker, intrusion detection systems etc.

Process/Procedure

* An outline of processes and procedures that should be followed within an investigation

Interviews/Investigations

* A list of who has been interviewed regarding the investigation including users, management etc., and how these testimonies will be acquired and used in the investigation.

Chain of Custody

* This will show the chronological documentation showing the seizure, custody, control, transfer, analysis and disposition of electronic evidence as required by law so that evidence may be upheld during litigation.

Examination

* This will outline the examination procedures and techniques used throughout the forensic process such as cross-drive analysis, live analysis, extraction of volatile data

Analysis

* This will outline the procedures and techniques used to analyze evidence and determine the who/what, where, when, how, and associated artifacts and metadata of the acquired data

Reporting

* This will outline the procedure of reporting forensic evidence in a way that effectively reflects the objective facts of the case in a manner that supports the case narrative

Recommendation

* This will outline the process of obtaining the views and experiences of the individuals involved in an investigation and how this information will be used to improve the handling of future investigations.