Technical Procedure for Target Drive Preparation

1.0 Purpose - The purpose of this procedure is to wipe all information from Target drives used in forensic casework in order to ensure that no data overlap occurs between cases.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory in preparing Target drives for use in forensic computer examinations.

3.0 Definitions

- **Target drive** – Drive to which information from the evidence drive is being written.
- **Wipe** – Permanently deleting all data from a drive by overwriting the data with a known value.

4.0 Equipment, Materials and Reagents

- Forensic Tower or Portable Forensic Workstation
- Hard Drive
- Approved software or hardware device for wiping data
- F-disk or G-disk software programs as necessary

5.0 Procedure

5.1 Select a Target drive that has sufficient storage capacity to hold the forensic image files and recovered files generated from the evidence hard drive.

5.2 Attach a label to the Target drive with pertinent case information.

5.3 Use an approved wipe utility or approved hardware device such as the VOOM Hardcopy II to remove all information from the drive.

5.4 Create a new primary partition on the Target drive.

5.5 Format the Target drive.

5.6 Enter a suitable name for the Target drive to ensure it will not be confused with other drives (e.g., forensic image, target, etc.).

5.7 Directories can be created on the drive in order to keep the evidence organized.

5.8 This procedure shall be used for new hard drives as well as hard drives use in previous cases.

5.9 When imaging a computer in the field, the Target drives shall be prepared by this procedure prior to arriving at the scene. This will speed the process of imaging the computer and will result in a shorter down time for the evidence computer.

5.10 Standards and Controls - A control disk image with a known hash value is used to ensure the proper functioning of forensic computers used in casework.

5.11 Calibration - The forensic towers used in casework shall be verified each day that they are used to ensure that the computer hardware and software are functioning properly (see the Computer Performance Verification Procedure).

5.12 Maintenance – N/A

5.13 Sampling - N/A

5.14 Calculations - N/A

5.15 Uncertainty of Measurement – N/A

6.0 Limitations - Failure to clean the information from a previously used hard drive can lead to the possibility of data overlap.

7.0 Safety - N/A

8.0 References

- EnCase Forensic User Manual
- EnCase Intermediate Analysis and Reporting Course Guide
- EnCase Advanced Computer Forensics Course Guide
- Forensic Toolkit User Guide
- Forensic Boot Camp Training Manual
- Computer Performance Verification Procedure

9.0 Records - N/A

10.0 Attachments - N/A

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document