Technical Procedure for System Image Restoration

1.0 Purpose - The purpose of this procedure is to restore system drives used in forensic casework to a default state 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 system drives for use in forensic computer examinations.

3.0 Definitions

- **System drive** – The drive that contains the operating system (OS).
- **System Image** – Backup of drive that is used to prepare forensic tower for beginning new case.

4.0 Equipment, Materials and Reagents

- Forensic Tower or Portable Forensic Workstation
- Hard Drive
- Approved software for creating and restoring system images
- Factory Restore Image on CD or DVD
- Previously created system image (if available)

5.0 Procedure

5.1 If a previously created system image is available, skip to step 5.5.

5.2 If no previously created system image is available, or updates to the default system image need to be made, use the original Restore Disk that came packaged with the Forensic tower or perform a fresh install of the operating system.

5.3 Install any software from the Approved Computer Software List to be included on System Image.

5.4 Use an approved backup utility to create an image of the system image and restore system drive.

5.5 Restore the system drive using the previously prepared system image.

5.6 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.

5.7 Calibrations - 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).

5.8 Maintenance – N/A

5.9 Sampling - N/A

5.10 Calculations - N/A

5.11 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

- Computer Performance Verification Procedure
- Approved Computer Software List

9.0 Records - N/A

10.0 Attachments – N/A

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document
10/31/2013	2	Added issuing authority to header