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 cross contamination 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 the system drive that contains a clean install of the operating system (OS).
- **Power-On Self Test (POST)** – A series of diagnostic tests that are performed when a computer powers on and determines proper functioning of the hardware components.

4.0 Equipment, Materials and Reagents

- Forensic Tower or Portable Forensic Workstation
- System Drive
- Approved software for creating and restoring system images
- Factory Restore Image
- 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 are required, then use the original Restore Disk that came packaged with the Forensic computer or perform a fresh install of the operating system.

5.3 Install any software from the Approved Software and Hardware for Computer Forensic Examinations List to be included on the system image.

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

5.5 Restore the system drive using the system image.

5.6 The Forensic Scientist shall ensure that the system drive restored properly and that the forensic computer completed its POST successfully after restore.

5.7 The case preparation notations shall be made in the worksheet/examiner's notes. The "Case Start" date shall be the day the case was initially started and when the case preparation process was completed.

5.8 **Standards and Controls -** All forensic computers and forensic tools shall be functioning properly prior to beginning a computer forensic examination (see Technical Procedure for Computer Forensics Performance Verification).

5.9 **Calibrations -** N/A

5.10 Maintenance – N/A

5.11 Sampling - N/A

5.12 Calculations - N/A

5.13 Uncertainty of Measurement - N/A

6.0 Limitations - Failure to restore the system drive after each case may lead to the possibility of cross contamination.

7.0 Safety - N/A

8.0 References

- Technical Procedure for Computer Forensics Performance Verification
- Approved Software and Hardware for Computer Forensic Examinations List

9.0 Records - N/A

10.0 Attachments – N/A

Revision History		
Effective Date	Version Number	Reason
12/02/2020	4	5.7 - The case preparation notations shall be made in the worksheet/examiner's notes. The "Case Start" date shall be the day the case was initially started and when the case preparation process was completed. Corrected header information

All copies of this document are uncontrolled when printed.