A. Purpose:

To outline the steps taken to ensure that a forensic computer being used to examine and store digital evidence is secure and working properly.

B. Responsibility:

Forensic examiners

C. Definitions/Abbreviations:

Refer to CC SOP-26 - Definitions and Abbreviations

D. Procedure:

1. Turn on the forensic computer and verify that the POST / boot sequence executes properly.
2. Ensure that the forensic computer requires a logon password for access.
3. Ensure that there is no case related material opened or accessible on the system and temporarily enable the internet network connection:

   Review operating system updates available and install if necessary.

   Ensure that the anti-virus and malware definitions have been updated.
4. Restart the system and verify that the POST / boot sequence executes properly; also verify that the operating system updates installed properly by reviewing the update history.
5. Disable the internet network connection on the forensic system.
6. In the event that verification of the system fails, resolve the issue before proceeding with any examinations using this computer.
7. Troubleshooting procedures include, but are not limited to the following:
   a. Training, knowledge and experience.
   b. Technical references.
   c. Consulting with co-workers and technical support.
8. If the issue cannot be resolved, the computer cannot be used for digital evidence analysis and a "Out of Service" sticker should be placed on the computer.
9. Document the verification process by documenting the verification date in the forensic system's maintenance log book along with a note that this check was performed..
10. A notation that software and/or hardware maintenance was performed on the system is to be recorded in the individual examiner's maintenance log book.
11. The system POST / boot sequence check, any necessary operating system updates and antivirus updates must be performed prior to starting a new case and/or following system repairs.

E. References:

1. Technical references