A. Purpose:

To outline the steps taken when previewing electronic evidence that has been submitted to the Computer Crimes Unit prior to or in place of full analysis while maintaining the integrity of the evidence.

B. Responsibility:

CCEEU forensic examiners.

C. Definitions:

Refer to CC SOP-26 - Definitions and Abbreviations.

D. Procedure:

1. Retrieve the evidence and update the chain of custody.
2. Prepare Laboratory Notes (QR-CC-5) for the submitted evidence. Record a description and /or relevant information about the evidence:

   Computer Information - Make, Model and Serial Number;

   Hard Drive Information - Subitem#, Make, Model, Serial Number, Interface Type, Manufacturer's Total Sectors and capacity;

   Removable media/Other - Subitem#, Make, Model, Serial Number, Media type, Manufacturer's capacity.
3. Initial the submission barcode label.
4. Use the Laboratory Notes (QR-CC-5) as a narrative to describe actions and observations made during the entire preview process.
5. If the submission is packaged, photograph, with a unique identifier present, the unopened package focusing on:
   a. Evidence labels and any other identifying markers
   b. Notable marks or damage
6. Remove the packaging.
7. Photograph, with a unique identifier present, the exterior of the computer focusing on:
   a. Top and front face
   b. Rear and all connectors
   c. Serial numbers, evidence labels and any other identifying markers
   d. Notable marks or damage
8. If applicable, open the computer case and note your access into the computer by putting the Laboratory Case Number, Submission Number and your initials on the frame inside the computer. In the event of a laptop or similar device, note your access inside the battery compartment. If not, locate a suitable place on the laptop exterior and record this information in your notes.
9. Photograph, with a unique identifier present, the interior of the computer focusing on:

a. Overall view of the inside of the computer
b. Location of the hard drive(s)
c. Close-up of the hard drive(s)
d. Anything notable inside the case

10. Remove power and data cables, if necessary, from the hard drive(s) and write the following on the cables to indicate the hard drive(s) that the cables were connected to:
    a. Your initials
    b. Hard drive designator (e.g. "HD1" for hard drive 1, "HD2" for hard drive 2)
11. Remove hard drive(s) and photograph, with unique identifier present, the hard drive(s) focusing on:
    a. Top of hard drive(s)
    b. Jumper settings
    c. Make, model, serial number, LBA and any other identifying markers
12. Note your access to the hard drive(s) with the following information transcribed on the hard drive(s):
    a. Laboratory Case Number
    b. Sub-item number following the naming convention below:
        Evidence Submission Number Hard Drive Number
        For example: S1_HD1.....S1_HD2.....
    c. Your initials
13. If applicable, sub-itemize evidence in LIMS; updating chain of custody.
14. If applicable, process the BIOS as follows:
    a. With hard drives removed from the computer connect the computer to a monitor and keyboard
    b. Turn the computer on
    c. Break into the setup screens by entering the appropriate keystrokes
    d. Record the appropriate BIOS information on the in the Laboratory Notes (QR-CC-5).
    e. In certain instances it may not be possible to gain access to the BIOS settings. In these cases, document any attempts made and make note in the Laboratory Notes (QR-CC-5) that attempts to access the BIOS were unsuccessful.
15. Connect the evidence drive or media to a forensic computer using an approved read-only hardware device or software. Document the make, model and serial#/Tag# of the write block / read-only hardware device using Laboratory Notes (QR-CC-5).
16. Conduct the preview examination using only approved software and established examination protocols.
17. Complete Laboratory Notes(QR-CC-5)/Analysis Notes (QR-CC-6).
18. Any hard drive, media or submitted evidence where a preview examination is conducted and found to contain items of evidentiary value must undergo a full forensic examination in order to

officially report out the positive findings. If a preview examination results in negative findings, (1) a full forensic examination may be conducted or (2) a statement that "only a preview examination was conducted on the evidence item with negative results" must be included in the final report.

19. Reassemble the computer leaving the data and power cables disconnected from the hard drive(s).
20. Repackage the computer if necessary.
21. If additional digital media was found, appropriately package it and adhere it to the computer or place it within the computer's packaging.
22. Update the chain of custody in JusticeTrax and return the computer to the evidence area.