DEUSOP12 - Handling Sensitive Media

Table of Contents

1. Scope

1.1. This standard operating procedure addresses how media that is deemed sensitive by Department of Forensic Sciences management due to subject matter, owner, affiliation or other rationale should be treated, handled, and stored in the laboratory.

2. Background

2.1. To establish the practices for documenting the examination of evidence to conform to the requirements of the Department of Forensic Sciences (DFS) Digital Evidence Unit *Quality Assurance Manual*, the accreditation standards under ISO/IEC 17025:2017, and any supplemental standards.

3. Safety

3.1. If necessary due to the condition of the media, wear personal protective equipment (e.g., lab coat, gloves, mask, eye protection), when carrying out standard operating procedures.

4. Materials Required

4.1. Storage media, encryption program, evidence tape, access to LIMS.

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

7.1. When digital evidence is received and deemed sensitive, document the media on the appropriate acquisition form. Unless identifying information required by the form is deemed sensitive, complete the form(s).

7.2. For creation of an image deemed sensitive, the image needs to be encrypted or placed in an encrypted container.

7.2.1. For encrypting an image, make sure the encryption option in the imaging software is enabled. Record the password for decryption on the acquisition form.

7.2.2. For placing an image in an encrypted container, create an encrypted partition on storage media. Record the password on the acquisition form. Create an image of the sensitive media and place within the encrypted container.

7.3. For examination of sensitive media, decrypt the image or place the image outside the encrypted container on a DEUNet forensic workstation. Complete DEUF05 – Forensic Examination. If any scope, methodology or results have been deemed sensitive, note on the form and provide an approved alternate method or media.

7.4. All completed forms, reports, notes and photographs should not be stored on DEUNet. All items should be saved to media, encrypted and stored with the Best Evidence copy.

7.5. Storage of sensitive media should be retained in the encrypted format/encrypted container within the DEU evidence room. It should be entered into LIMS per DEUSOP05 – Digital Device Acquisition. Password for encrypted files should be stored in LIMS in the notes of the evidence item(s).

7.6. No working copy of the sensitive media will be stored on DEUNet, unless instructed by management due to necessity. On the acquisition form, this will be indicated by “not created per SOP” or other indication that no working copy has been saved.

7.7. Access to the Best Evidence copy is restricted to employees with access to the DEU evidence storage.

7.8. Disposition of the sensitive media's original evidence will be taken on a case-by-case basis. Unless instructed by DFS management, DEU will not retain the original evidence in the DEU evidence storage.

8. Sampling

8.1. Not applicable.

9. Calculations

9.1. Not applicable.

10. Uncertainty of Measurement

10.1. Not applicable.

11. Limitations

11.1. Due to damage or other factors, some or all of the above examinations might not be possible. It is at the discretion of the analyst as to what examinations are necessary and if they should be conducted.

12. Documentation

12.1. DEUSOP05 – Digital Device Acquisition

12.2. DEUF05 – Forensic Examination Form

13. References

13.1. Digital Evidence Unit Quality Assurance Manual (Current Version).

13.2. DFS Departmental Operations Manuals (Current Versions).

13.3. Forensic Science Laboratory (FSL) Laboratory Operations Manuals (Current Versions).

13.4. Digital Evidence Unit Laboratory Operations Manuals (Current Versions).

13.5. SWGDE Comments on Forced Minimization Requirements for the Seizure of Digital Evidence (v1.0 October 8, 2016).