

IOCE Principles and Definitions

Principles

1. Upon seizing digital evidence, actions taken should not change that evidence.
2. When it is necessary for a person to access original digital evidence, that person must be forensically competent.
3. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
4. An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence in their possession.
5. Any agency, which is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Definitions

Digital Evidence

- *Information stored or transmitted in binary form that may be relied upon in court.*

Original Digital Evidence

- *Physical items and those data objects, which are associated with those items at the time of seizure.*

Duplicate Digital Evidence

- *A duplicate is an accurate digital reproduction of all data contained on the original physical item.*

Copy

- *A copy is an accurate reproduction of information contained in the data objects independent of the original physical item.*