



**FIRST RESPONDERS GOOD PRACTICE GUIDE TEMPLATE**

**14-12-2000**

**Introduction**

Law enforcement around the world will benefit from the adoption of good practice guides for first responders to crime scenes that involve computer evidence. The good practice guides established by the country or agency should set minimum procedures for the handling of this type of evidence. IOCE recognises however that good practices involve more than what is suggested in this document, including concerns for establishing a chain of custody and compliance with local procedures and laws.

The information provided here should serve as a template to assist law enforcement agencies in developing a document which gives a basic understanding of key technical and legal factors regarding searching and seizing electronic storage devices and media according to the principles recommended by the G8.

IOCE suggests that it may be appropriate to issue a good practices guide that provides in-depth considerations. Additionally, it may be appropriate for law enforcement agencies to issue a guide in a smaller format that provides an easily accessible overview of good practices for first responders on the street. This smaller version of the guide would be similar in format to one that could be carried as a small pocket reference. Noted below by the designation “[PV]” (for “Pocket Version”) are portions of this template that IOCE recommends should be included in the small pocket version of a good practices guide.

**Principles Recommended by G8**

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

**CAVEAT -**

It is important that you make the first responder aware of the need for them to recognise their limitations in their capabilities of handling digital evidence. Often times a first responder may not be able to obtain the assistance of an expert in the handling of computer evidence. In such circumstances the first responder needs to act as best possible to preserve computer evidence with the understanding that evidence may be damaged or lost in the process. This may need to be accepted as inevitable in view of the speed with which technology advances. It is hoped that the adoption of a good practices guide will minimise the potential adverse consequences from the lack of availability of the expert to the first responder.

**Chapter – Recognition of sources of electronic evidence**

1. Look at computer equipment (other devices to be handled by other groups) – why can it be relevant (so it’s not overlooked) – possible inclusion of photographs (inclusion more important than exclusion regardless of dated material) – descriptions of types of evidence – include media – include networks
2. Included in here should be a description as well as photo of commonly encountered computer evidence such as computer systems, components, memory cards, scanners, printers, modems, network

components, cables and connectors, hard drives, removable storage devices and media, pagers, digital cameras, handheld devices, telephones, answering machines, access control devices, etc. (should be additional updates on a regular basis)

### **Chapter - Interrogation examples**

A good practices guide should include guidance for the first responder in making an initial inquiry of witnesses about computer evidence. The areas of inquiry will vary from case to case but may include some of the following:

1. Ownership
2. Users
3. Physical locations/backups – locations of servers, and other points of access
4. Passwords – phrases - BIOS passwords
5. System administrators and contractors
6. Hardware configurations
7. Networks - ask questions in relation to system administrators – wireless networks
8. Telecomm connections
9. Use of cryptography

### **Chapter – Tools and Equipment**

Special tools and equipment may be required to collect electronic evidence. First responders may not necessarily have in their possession a complete toolkit but rather should have access to adequate tools through their agency. A good practices guide should include details about the tools and equipment required by the local agency such as:

1. Toolkit
2. Documentation tools
3. Disassembly and removal
4. Package and Transport – sealing equipment (wax, tape, etc)
5. Other items
6. [PV – no detail – small camera, marker]

### **Chapter – Preserving the Evidence**

- The scene:
  1. Secure and evaluate the scene
  2. Protect perishable data and integrity – limited battery life
  3. Conduct preliminary interviews
  4. Take control of the scene – remove people from computers and power supply
- Documenting the scene:
  1. Photographing
  2. Diagramming
  3. Identifying different components
  4. Document personnel
  5. Document the equipment's status – what's visible, etc.
  6. Physical security
  7. Important information contained on documents – post-it notes, etc.
- Packaging procedure
- Transportation procedure
  1. Keep away from magnets, radio transmitters and otherwise hostile environments.
- Storage procedure

[PV – include bag and tag information – need to account for situations where no packaging is big enough – handle according to your local policies]

## **Chapter – Evidence collection**

[PV – less detail but include – focus on do's and don'ts]

1. handle carefully to preserve evidentiary value/chain of custody
2. consider trace evidence – fingerprints, etc.
3. recovery of non-electronic evidence
4. collecting standalone/laptop computer –
  - A. if off leave it off
  - B. if on:
    - a. consult expert
    - b. if expert not available:
      1. photograph screen, disconnect all power sources by unplugging from the computer and then from the wall – if laptop, remove all batteries
      2. photograph/diagram and label back of computer components with existing connections
      3. label all connectors/cable ends to allow reassembly as needed
  - C. take all components, including power supplies, etc
5. Networks, mainframes – computers in a complex environment – this is where the line of limitation should be drawn – expert assistance should be sought
6. Other devices and peripherals – digital cameras

Special Note: Pulling the plug or removing the battery could cause damage to or destroy potential evidence. In some situations there may be no viable alternative. IOCE recognises that there is a lot controversy regarding this subject. Policy should be established according to your local guidelines. The reasoning as to the policy you set should be included in your guideline. (Why?)

## **Chapter – Resources**

[PV – including this information is up to local agency]

1. Country or department resource guide
2. Glossary of terms (not to include in small guide)
3. Legal resources – web sites, etc.(not to include in small guide)
4. Technical resources – other technical resources accessible within your locality (not to include in small guide) [PV – local phone numbers as required]

## **Chapter – References**

[PV – reference larger guide]

(include as needed by local jurisdiction?)

## **Conclusion**

A good practices guide can be both a practical and a training resource depending on how it is written. In certain circumstances it may be appropriate to provide an explanation as to why specified procedures should be followed.