IT Forensic Evidence Collection Procedure Sample

1. Purpose

This document outlines the standard procedures for the collection, preservation, and documentation of digital evidence during IT forensic investigations.

2. Scope

Applicable to all IT forensic investigations conducted by authorized personnel within the organization.

3. Responsibilities

- **Forensic Investigator:** Responsible for evidence identification, collection, preservation, documentation, and chain-of-custody.
- **IT Support:** Assists in identifying affected systems and facilitating access.
- **Management:** Ensures adherence to the evidence collection policy.

4. Evidence Collection Steps

1. **Preparation**
   - Obtain authorization for forensic investigation.
   - Prepare documentation forms and forensic equipment (e.g., write blockers, collection devices).

2. **Identification**
   - Identify all systems and storage devices that may contain relevant evidence.
   - Photograph hardware and work area if necessary.

3. **Preservation**
   - Ensure devices are not tampered with prior to collection.
   - Disconnect devices if required, following proper shutdown procedures.

4. **Collection**
   - Use forensic tools and write blockers for data acquisition.
   - Create bit-for-bit images/clones of storage media.
   - Label devices and collected images with unique identifiers.

5. **Documentation**
   - Record details on evidence collection forms (time, date, device, serial number, handler).
   - Maintain a chain-of-custody log for all evidence collected.

6. **Transport and Storage**
   - Securely transport physical and digital evidence to designated storage.
   - Limit access to authorized personnel only.

5. Chain of Custody Log Example

Date/Time	Handler	Evidence ID	Description	Action	Signature
2024-06-01 10:17	John Doe	DEV001	Laptop - Dell Precision 5550	Collected	

2024-06-01 12:20	Jane Smith	IMG001	Disk Image - DEV001	Acquired & Stored	

6. Documentation

All activities must be thoroughly documented to ensure evidence integrity and admissibility. Use standard forms provided in Appendix A for evidence logs and chain-of-custody.

7. Appendix A: Sample Evidence Collection Form

Evidence ID	Date/Time	Description	Location	Handler	Remarks

End of Document