Evidence Collection Format

Security Breach Investigation Report

Date of Collection

Time of Collection

Collected By

Investigator Name and Designation

Contact Information

Email / Phone

Location of Evidence

Physical/Network Location

1. Evidence Details

Type of Evidence

e.g., Log File, Device, Hard Drive

Evidence Reference Number

Unique Reference

Description

Brief description of the evidence

Associated Incident ID

Link to Security Incident

2. Collection Process

Method of Collection

Describe the tools and techniques used

Chain of Custody

Record of individuals who handled the evidence

Preservation Measures

Steps taken to protect evidence integrity

3. Evidence Analysis (If Applicable)

Initial Findings

Observation at the time of collection or analysis

Remarks

Any additional comments

4. Witnesses (If Any)

Names and Contact

List witnesses and their contacts

5. Attachments

List of Attached Files / Evidence (photos, screenshots, logs, etc.)

List and describe all attached evidence

Signature of Collector

Name / Signature

Date

Important Notes:

- Document all evidence handling steps in chronological order to maintain chain of custody.
- Ensure evidence is preserved in its original state to maintain integrity and admissibility.
- Access to evidence should be restricted to authorized personnel only.
- All fields should be as detailed and accurate as possible to support the investigation.
- This document may be used in internal investigations and legal proceedings.