Cyberattack Evidence Collection Checklist

1. Initial Information

□ Record date and time of incident detection

□ Note how incident was reported/discovered

□ Document affected systems/applications

□ List contacts and personnel involved

2. Evidence Preservation

□ Preserve volatile data (memory, running processes, network connections)

□ Isolate affected systems (if necessary)

□ Create forensic disk images

□ Start chain-of-custody documentation

3. Data Collection

□ Collect system, network, and application logs

□ Gather suspicious files or binaries

□ Archive relevant communications (emails, messages)

□ Retrieve network traffic captures (if available)

4. Documentation

□ Log all investigative actions taken

□ Maintain a timeline of events

□ Take photographs/screenshots if necessary

5. Additional Notes & Observations

□ Record any additional observations