# Task 2: Evidence Collection Policy

## Scenario

After the recent security breach, Always Fresh decided to form a computer security incident response team (CSIRT). As a security administrator, you have been assigned the responsibility of developing a CSIRT policy that addresses incident evidence collection and handling. The goal is to ensure all evidence collected during investigations is valid and admissible in court.

Consider the following questions for collecting and handling evidence:

1. What are the main concerns when collecting evidence?
2. What precautions are necessary to preserve evidence state?
3. How do you ensure evidence remains in its initial state?
4. What information and procedures are necessary to ensure evidence is admissible in court?

## Tasks

Create a policy that ensures all evidence is collected and handled in a secure and efficient manner. Remember, you are writing a policy, not procedures. Focus on the high-level tasks, not the individual steps.

Address the following in your policy:

* Description of information required for items of evidence
* Documentation required in addition to item details (personnel, description of circumstances, and so on)
* Description of measures required to preserve initial evidence integrity
* Description of measures required to preserve ongoing evidence integrity
* Controls necessary to maintain evidence integrity in storage
* Documentation required to demonstrate evidence integrity

## Required Resources

* Internet access
* Course textbook

## Submission Requirements

* Format: Microsoft Word (or compatible)
* Font: Arial, size 12, double-space
* Citation Style: Follow your school’s preferred style guide
* Length: 3 pages

## Self-Assessment Checklist

* I created a policy that addressed all issues.
* I followed the submission guidelines.