# Example Workflow: Responding to a Malware Infection

---

**1. Policy: Incident Response Policy**

- **Purpose**: Define how the organization will respond to security incidents, including malware infections.
- **Key Points**:
  - Report incidents immediately to the IT department.
  - Follow the incident response process (detection, containment, eradication, recovery, post-incident review).

---

**2. Procedure: Malware Incident Response Procedure**

- **Purpose**: Provide step-by-step instructions for responding to a malware infection.
- **Steps**:
  1. **Detection**:
     - Monitor systems for signs of malware (e.g., unusual pop-ups, slow performance).
     - Use antivirus software to scan for malware.
  2. **Containment**:
     - Disconnect the infected device from the network.
     - Disable shared drives and remote access.
  3. **Eradication**:
     - Use antivirus software to remove the malware.
     - Patch vulnerabilities that allowed the malware to infect the system.
  4. **Recovery**:
     - Restore files from backups.
     - Verify that the system is clean and functioning properly.
  5. **Post-Incident Review**:
     - Analyze how the malware entered the system.
     - Update the incident response plan to prevent future infections.

---

### 3. Standard: Malware Protection Standard

- **Purpose**: Define requirements for protecting systems from malware.
- **Requirements**:
  - Install and regularly update antivirus software on all devices.
  - Enable real-time scanning and automatic updates.
  - Restrict users from installing unauthorized software.

---

### 4. Protocol: Malware Scanning Protocol

- **Purpose**: Provide detailed instructions for scanning systems for malware.
- **Steps**:
  1. Open the antivirus software.
  2. Initiate a full system scan.
  3. Review the scan results for detected threats.
  4. Quarantine or remove any identified malware.
  5. Generate a report of the scan results.

---

## Workflow in Action

### Scenario

An employee reports that their computer is running slowly and displaying unusual pop-ups. The IT department suspects a malware infection.

---

### Step 1: Detection

- **Action**: The IT department uses the **Malware Scanning Protocol** to scan the employee’s computer.
- **Outcome**: The scan detects a malware infection.

---

### Step 2: Containment

- **Action**: Following the **Malware Incident Response Procedure**, the IT department disconnects the infected computer from the network and disables shared drives.
- **Outcome**: The malware is prevented from spreading to other systems.

---

**Step 3: Eradication**

- **Action**: The IT department uses the **Malware Scanning Protocol** to remove the malware and applies patches to fix vulnerabilities.
- **Outcome**: The malware is removed, and the system is secured.

---

**Step 4: Recovery**

- **Action**: The IT department restores files from backups and verifies that the system is clean and functioning properly.
- **Outcome**: The employee’s computer is restored to normal operation.

---

**Step 5: Post-Incident Review**

- **Action**: The IT department analyzes how the malware entered the system and updates the **Incident Response Policy** and **Malware Protection Standard** to prevent future infections.
- **Outcome**: The organization is better prepared to handle similar incidents in the future.