**SOP for Virus or Malware Detection**

**Purpose**

To prevent and mitigate security threats caused by malware or viruses.

**Scope**

Covers all devices connected to the corporate network.

**Procedure**

1. **User reports suspicious activity or malware alert.**
2. Isolate infected system from network.
3. Perform full antivirus/malware scan.
4. Remove/quarantine infected files.
5. Apply necessary patches and security updates.
6. Escalate to IT Security if a major breach is detected.
7. Confirm resolution and close the ticket.