

# Data Loss & Malware Threats SOP

## Purpose:

---

This document outlines the SOP for implementing security measures to protect the system, user data, and sensitive information from unauthorized access, malware infections, and potential data loss incidents.

## Scope:

---

This SOP is to be used for the guidelines and procedures we have set for securing Windows 10 endpoint workstations, ensuring the confidentiality, integrity, and availability of data.

## Responsibilities:

---

The IT department at Team Knonsense is responsible for the implementation, maintenance and review of this policy.

## Prerequisites:

---

- A. The IT department at Team Knonsense is responsible for the implementation, maintenance and review of this policy. This will only be done by the IT department, following our set SOP.
- B. [SOPs](#)

## Procedure:

---

It is important to conduct periodic security audits to assess the effectiveness of implemented security measures. Review logs, perform vulnerability scans, and analyze system configurations to identify and address any potential vulnerabilities or gaps.

Implementing security measures is an ongoing process that requires regular maintenance, updates, and user awareness.

1. Update Windows
  - Enable automatic updates or regularly check for updates manually.
2. Windows Virus and Threat Protection

- Enable and perform regular scans to detect and remove any malware.
- 3. Enable and Configure Windows Firewall
  - Allow only necessary applications and services through the firewall.
- 4. Implement Strong Password Policies
  - Enforce strong password policies for user accounts and encourage users to create unique and complex passwords and periodically change them.
- 5. Perform Regular Data Backups
  - Refer to [Backup and Restore user data, critical infrastructure configurations and hosted data SOP](#)
- 6. Enable User Account Control (UAC)
  - Adjust the UAC settings to an appropriate level of security based on organizational needs.
- 7. Update Applications
  - Apply patches and updates provided by the software vendors to address security vulnerabilities.

## References:

---

- <https://www.thewindowsclub.com/windows-defender-security-center>

## Definitions:

- Malware - Malicious Software

## Revision History:

---

5/16/2023 - Adrian Mundo

5/16/2023 - Raphael Chookagian