# Standard Operating Procedure

**PURPOSE: Secure Windows 10 endpoint workstations from data loss and malware threats**

I. **Introduction**: Our organization recognizes the increasing sophistication of cyber threats and the importance of safeguarding our digital assets. This SOP aims to establish a robust framework for securing Windows 10 endpoint workstations, which are pivotal in our daily operations.

**A. Required Training**

- Familiarity using windows 10 operating system
- Understanding the basic of backup and recovery process
- Familiarize yourself with built-in Windows 10 backup features like File History and Windows Backup.

**B. Administrative Procedures**

- Knowledge on recovery strategy and tools
- Documentation and communication
- Ensuring business continuity in the event of disaster/threats,etc

**C. Description of Laboratory**

- Hardware and software engineers
- Large garage space

**D. General Laboratory Safety**

- Clearly label and communicate any potential hazards associated with specific equipment.
- Conduct regular fire drills to ensure employees are familiar with evacuation procedures.
- Encourage a culture of safety awareness and reporting.

II. **Procedures:**

- **Safety Awareness Training**:
  - ☐ Safety/Training meetings every Monday
  - ☐ hazard or suspicious activity reports

- **AntiVirus and Anti Malware Software**:
  - ☐ Install reputable antivirus and anti malware software tools on endpoint

- ☐ Make sure all software is up to date and ready to defend for latest threats
- ☐ Regularly check/install updates/upgrades on windows

- **Endpoint security policies**:
  - ☐ Establish and enforce endpoint security policies to regulate user activities, software installation and system configurations.
  - ☐ Admin privileges and restrict unnecessary access

- **Firewall Configuration**:
  - ☐ Configure and enable the Windows Defender and firewall and PFSense in the events of Virtualbox
  - ☐ Establish rules to block unauthorized use
- **Security monitoring**:
  - ☐ Ensure that the network connections are secured with strong encryption and strong passwords
  - ☐ Regularly review security logs and alert

- **Documentation and reporting**:
  - ☐ Maintain detailed documentation of security configurations, policies, and incidents
  - ☐ Generate regular reports on security status of Windows 10 workstations and management review

## III. Definitions:

- Malware - Software intended to damage a computer, mobile deceive, operating system or to take over control of computer functions
- Data loss - Error condition in information systems that occur during a disaster or a power outage, spilled liquid, hard drive failures, etc. When important or private information can not be retrieved.
- Windows 10 - An operating system to navigate through computers and networks.
- Endpoint user - Device or node that is connected to the LAN or WAN and accepts communications back and forth across the network.

## IIII. References:


- https://learn.microsoft.com/en-us/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10

Signature _____ Annual Review Date _____

APPENDICES