Standard Operating Procedure (SOP): Securing Windows 10 Endpoint Workstations from Data Loss and Malware Threats

1. Purpose:
The purpose of this SOP is to establish a standardized process for securing Windows 10 endpoint workstations from data loss and malware threats. This ensures the protection of sensitive information, maintains the integrity of systems, and mitigates the risk of security breaches.

2. Scope:
This SOP applies to all personnel responsible for managing and securing Windows 10 endpoint workstations within the organization.

3. Responsibilities:
- IT Security Team: Responsible for implementing security measures, monitoring threats, and enforcing security policies.
- IT Support Team: Responsible for providing technical assistance and support related to security measures on Windows 10 workstations.
- End Users: Responsible for adhering to security policies and guidelines to ensure the protection of their workstation.

4. Prerequisites:
- Understanding of Windows 10 security features and configuration options.
- Awareness of potential data loss and malware threats.

5. Procedures:

5.1. User Education and Awareness:
- Conduct regular user training programs to educate end users on security best practices, including password management, email and web browsing safety, and recognizing social engineering attacks.
- Communicate the importance of adhering to security policies and guidelines to all end users.

5.2. Endpoint Protection Software:
- Install and regularly update reputable antivirus and anti-malware software on all Windows 10 workstations.
- Configure the software to perform regular scans and real-time monitoring to detect and mitigate potential threats.

5.3. Windows 10 Updates and Patches:
- Enable automatic Windows Update settings on all workstations to ensure the installation of critical security updates and patches.
- Regularly review and test Windows updates before deployment to prevent compatibility issues.

5.4. Secure Configuration and Access Controls:
- Implement strong password policies and enforce the use of complex, unique passwords for user accounts on Windows 10 workstations.
- Enable multi-factor authentication where possible to enhance security.
- Limit user privileges to prevent unauthorized system modifications or installations.

5.5. Data Backup and Recovery:

- Establish a regular backup schedule to safeguard critical data on Windows 10 workstations.
- Use secure backup solutions, such as cloud-based or encrypted external storage, to protect against data loss due to hardware failure, malware attacks, or accidental deletion.

5.6. Web Filtering and Firewall:

- Implement web filtering measures to block access to malicious or inappropriate websites from Windows 10 workstations.
- Enable and configure the Windows Firewall to control inbound and outbound network traffic, minimizing the risk of unauthorized access.

5.7. Data Encryption:

- Enable BitLocker or a suitable disk encryption solution on Windows 10 workstations to protect sensitive data in case of device theft or unauthorized physical access.

5.8. Security Monitoring and Incident Response:

- Implement monitoring systems to track and log security events on Windows 10 workstations.
- Establish an incident response plan to promptly address and mitigate any security incidents or breaches.

6. References:

- Organization's security policies and guidelines.
- Microsoft documentation on Windows 10 security best practices.

7. Definitions:

- Endpoint Workstation: A Windows 10-based computer used by an individual for work purposes.

8. Revision History:

- Version 1.0: [17MAY2023] - [David Siebert]
  - Initial draft of the SOP.
- Version 1.1: [Date] - [Contributor Name]
  - Incorporated feedback from stakeholders.
  - Added section on security monitoring and incident response.