SOP: Securing Windows 10 Endpoint Workstations from Data Loss and Malware Threats

---

Objective:

The objective of this Standard Operating Procedure (SOP) is to outline the steps for securing Windows 10 endpoint workstations from data loss and malware threats. By following this SOP, we aim to protect sensitive data, maintain system integrity, and minimize the risk of malware infections.

Scope:

This SOP applies to all Windows 10 endpoint workstations within the organization.

Procedure:

1. Implement User Awareness Training:
    - Conduct regular training sessions to educate users about safe computing practices, including the risks of data loss and malware.
    - Train users on identifying and avoiding phishing emails, suspicious websites, and downloads from untrusted sources.
    - Promote the use of strong and unique passwords and the importance of regularly updating them.
2. Keep Windows 10 Up-to-Date:
    - Enable automatic updates on all workstations to ensure they receive the latest security patches and bug fixes from Microsoft.
    - Regularly check for and install Windows updates manually if automatic updates are not enabled or if critical updates are pending.
3. Deploy Endpoint Protection Software:
    - Install reputable antivirus and anti-malware software on all workstations.

- Configure the software to automatically update virus definitions and perform regular system scans.
- Ensure real-time scanning is enabled to detect and block potential threats in real-time.

4. Enable Windows Defender Firewall:
    - Enable and configure the built-in Windows Defender Firewall to control incoming and outgoing network traffic.
    - Set appropriate firewall rules to allow necessary network communication while blocking unauthorized access.
5. Enable Windows Defender SmartScreen:
    - Enable Windows Defender SmartScreen to provide protection against malicious websites and downloads.
    - Configure SmartScreen to block unrecognized apps and warn users about potentially harmful websites.
6. Implement Least Privilege:
    - Follow the principle of least privilege by granting users the minimum required access privileges.
    - Regularly review and adjust user permissions to ensure they align with their job responsibilities.
7. Enable BitLocker Encryption:
    - Implement BitLocker full-disk encryption to protect sensitive data on workstations.
    - Enable pre-boot authentication to ensure that only authorized users can access the encrypted data.
8. Regular Data Backups:
    - Establish a regular data backup policy to ensure critical files are backed up to a secure location.
    - Use automated backup solutions or cloud services to simplify the backup process and ensure data integrity.
9. Implement Web Filtering:
    - Deploy web filtering solutions to block access to known malicious websites and inappropriate content.
    - Configure web filters to restrict access based on organizational policies and guidelines.
10. Monitor and Respond:
    - Implement centralized logging and monitoring solutions to detect and respond to security incidents promptly.
    - Regularly review security logs for any suspicious activities or signs of malware infections.
    - Establish an incident response plan to outline the steps to be taken in the event of a security incident or breach.
11. Regular Security Audits:

- Conduct periodic security audits of Windows 10 workstations to identify vulnerabilities and ensure compliance with security policies.
- Perform vulnerability assessments and penetration testing to evaluate the effectiveness of security controls.

12. Regular Training and Awareness Updates:
    - Provide regular training updates and reminders to employees regarding security best practices and emerging threats.

References:

- Microsoft Windows Security Documentation
- Industry best practices for endpoint security

Revision History:

5/15/2023- SOP Securing Windows 10 Endpoint Workstations from Data Loss and Malware created by carlos rojas