SCD for Operating Systems for Saral

1. Introduction: This System Configuration Document (SCD) outlines the operating systems used by ABC Limited and their respective configurations. The operating systems play a critical role in the organization's technology infrastructure, and it is important that they are configured and maintained properly to ensure optimal performance and security.

2. Operating Systems: The following operating systems are used by ABC Limited:

a. Windows: Windows is the primary operating system used by ABC Limited for desktop and laptop computers. Windows is used for office productivity, communication, and other general-purpose applications.
b. MacOS: MacOS is used by ABC Limited for select employees who require a Mac-based operating system for their job duties. MacOS is used for graphic design, video editing, and other specialized applications.
c. Linux: Linux is used by ABC Limited for servers and other specialized applications. Linux is known for its stability, security, and versatility, making it an ideal choice for certain applications.

3. Configuration: The following configurations are applied to the operating systems used by ABC Limited:

1. Windows: Windows is configured with the latest security updates and patches. Antivirus software is installed on all Windows computers to protect against malware and other threats.
2. MacOS: MacOS is configured with the latest security updates and patches. Antivirus software is installed on all MacOS computers to protect against malware and other threats.
3. Linux: Linux is configured with the latest security updates and patches. Firewalls and other security measures are implemented to protect against unauthorized access and other threats.

4. Maintenance: The operating systems used by ABC Limited must be regularly maintained to ensure optimal performance and security. This includes installing software updates and patches, conducting system backups, and monitoring for security threats.

5. User Access: User access to the operating systems must be controlled and monitored to ensure that only authorized personnel have access to sensitive information. The IT department must implement user access control measures such as setting up user accounts, assigning roles and privileges, and periodically reviewing user access logs.

6. Disaster Recovery Plan: The IT department must have a disaster recovery plan in place to ensure that the operating systems can be quickly restored in the event of a disaster. This includes regular backups of the operating systems, hardware, and data.

7. Review: The operating systems used by ABC Limited must be regularly reviewed to ensure that they are configured and maintained properly. This includes conducting security audits, monitoring performance, and identifying areas for improvement.