OPERATING SYSTEM

Standard Control Document for Operating System in a Company

1. Introduction

This Standard Control Document (SCD) outlines the procedures for managing and maintaining the operating systems within the company.
The purpose of this SCD is to ensure that the company's operating systems are secure, reliable, and up-to-date.

2. Scope

This SCD applies to all computers and servers within the company, regardless of the operating system used.

3. Operating System Management

- The company will only use approved operating systems, which have been tested and validated for security, reliability, and performance.
- The operating systems will be kept up-to-date with the latest security patches and software updates.
- Regular backups of the operating system and critical data will be performed to ensure data recovery in the event of a system failure.

4. Operating System Security

The company will implement and enforce policies and procedures to protect the operating systems from security threats, such as viruses, malware, and hacking.
Antivirus software will be installed and kept up-to-date on all computers and servers.
Firewalls will be used to secure the network and protect the operating systems from external threats.

5. Password Policy

Passwords must be at least 8 characters in length and contain a combination of upper and lowercase letters, numbers, and special characters. Passwords must be changed every 90 days.

Passwords must not be reused for at least 12 months.

6. Anti-Virus Software

The company will use anti-virus software to protect its systems from viruses and other malicious software. The anti-virus software must be updated regularly to ensure that it is effective against the latest threats.

7. Software Updates

The company will use software updates to keep its systems up to date and to address any security vulnerabilities. Software updates must be installed promptly to ensure that the systems are protected from known security vulnerabilities.

8. Data Backup

The company will back up its data regularly to ensure that it is protected in the event of a data loss. The data backup must be stored in a secure location and must be tested regularly to ensure that it can be restored if necessary.

9. Firewall

The company will use a firewall to protect its network and systems from unauthorized access. The firewall must be configured to only allow traffic from trusted sources and to block traffic from untrusted sources.

10. Operating System Configuration

- The company will establish and maintain standard configurations for all operating systems, including hardware and software configurations.
- The standard configurations will be documented and updated regularly to ensure that all computers and servers are configured consistently and securely.

- Any changes to the operating system configurations will be approved by the IT department and documented in the change management process.

11. Operating System Monitoring

The IT department will monitor the operating systems on a regular basis to ensure their security and performance. The IT department will also monitor for any security threats, such as viruses or hacking attempts, and take appropriate action to mitigate any risks.

12. Operating System Incident Management

- In the event of an operating system incident, the IT department will follow the company's incident management procedures to resolve the issue.
- The IT department will document the incident, including the cause, resolution, and any lessons learned.
- The incident management process will be reviewed regularly to identify opportunities for improvement and to ensure that operating system incidents are handled consistently and effectively.

13. Conclusion

The SCD for operating system management provides a framework for managing and maintaining the company's operating systems, ensuring that they are secure, reliable, and up-to-date. By following this SCD, the company can reduce the risk of operating system incidents and ensure the continued availability and performance of its computer systems.