


IT STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh				
TITLE:	Network Configuration				
SOP No. 1.0.7	Issue Date	Effective Date	Review Due	Copy No.	Page 1 of 5

1.0.7 Network Configuration

1. PURPOSE

Ensure a standardized and secure network configuration across all systems and devices within DBL GROUP IT infrastructure.

2. SCOPE

This SOP applies to all network devices, including routers, switches, firewalls, servers, and end-user devices connected to the DBL GROUP IT Enterprise network.

3. Responsibility

The IT department is responsible for implementing and maintaining the network configuration standards outlined in this SOP.

4. Procedure:

4.1 Documentation


- Maintain an up-to-date inventory of all network devices.
- Document / Backup the current configuration settings of each network device.
- Store configurations in a secure location with version control.

4.2 Access Control:

- Implement strong access controls for network devices.
- Use unique usernames and complex passwords.
- Enforce the principle of least privilege.
(See Reference SOP 1.0.2)

4.3 Firewall Configuration:

- Regularly review and update firewall rules.
- Restrict unnecessary incoming and outgoing traffic.
- Document and justify any changes to firewall rules.
(See Reference SOP 1.0.23)

IT STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh				
TITLE:	Network Configuration				
SOP No. 1.0.7	Issue Date	Effective Date	Review Due	Copy No.	Page 2 of 5

4.4 Router and Switch Configuration:

- Configure router and Switch as per approved design.
- Use standard naming conventions for routers and switches.
- Implement VLANs to segment network traffic.
- Disable unnecessary services and interfaces. (See Appendix-A)

4.5 Security Patch Management:

- Regularly update firmware and software on network devices.
- Apply security patches promptly.
- Schedule maintenance windows for updates to minimize disruptions.

4.6 Monitoring and Logging:

- Implement network monitoring tools to track performance and detect anomalies.
- Enable logging on network devices.
- Regularly review logs for security incidents and performance issues.

4.7 Wireless Network Configuration:

- Secure wireless networks with WPA3 encryption.
- Change default SSIDs and passwords.
- Implement guest networks with restricted access.

4.8 Backup and Recovery:

- Regularly backup network device configurations.
- Store backups in a secure offsite location.
- Test the restoration process periodically.


4.9 Network Segmentation:

- Segment the network based on sensitivity and functionality.
- Use firewalls and access controls to regulate traffic between segments.
- Isolate critical systems to enhance security.

4.10 Incident Response:

- Develop and document an incident response plan for network security events.
- Train IT staff on incident response procedures.
- Regularly conduct tabletop exercises to test the incident response plan.

5. DOCUMENTATION AND RECORD-KEEPING

IT STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh				
TITLE:	Network Configuration				
SOP No. 1.0.7	Issue Date	Effective Date	Review Due	Copy No.	Page 3 of 5

- a. Maintain detailed records of user access requests, approvals, and modifications.
- b. Keep an inventory of users with access to sensitive systems and data.
- c. Retain access logs for a specified period as per organizational policy.

ABBREVIATIONS

SOP	-	Standard Operating Procedure
IT	-	Information Technology

1. Legal Compliance:

Ensure that roles and responsibilities outlined in the SOP comply with legal and regulatory requirements. This is particularly important in areas such as labor laws, data protection, and workplace safety.

2. Communication:

Clearly communicate the SOP to all relevant stakeholders. Ensure that employees are aware of their roles and responsibilities and understand the implications of not adhering to them.


3. Accessibility:

Make the SOP easily accessible to all relevant personnel. This could involve storing it in a central repository, such as an intranet or document management system.

ASSOCIATED DOCUMENTS

REFERENCES

- 9.1 FDA's 21 CFR Part 11: Electronic Records; Electronic Signatures
- 9.2 GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems
- 9.3 Industry best practices

IT STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh				
TITLE:	Network Configuration				
SOP No. 1.0.7	Issue Date	Effective Date	Review Due	Copy No.	Page 4 of 5


APPENDICES

APPENDIX-A	User Authorization Form
APPENDIX-B	
APPENDIX-C	
APPENDIX-D	
APPENDIX-E	

REVISION HISTORY

REVISION DATE	REVISION NUMBER	DESCRIPTION OF REVISION
30 Jan' 24	01	First edition of the SOP

Prepared by:	Signature	Date
Name: Md. Atiqur Rahman		
Designation: Manager		
Reviewed by:	Signature	Date
Name: Md. Imrul Hasan		
Designation: Sr. Manager-IT		
Approved by:	Signature	Date
Name: Zahidul Alam		
Designation: CIO		
Authorized by:	Signature	Date
Name:		
Designation:		

IT STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh					
TITLE:	Network Configuration					
SOP No. 1.0.7	Issue Date	Effective Date	Review Due	Copy No.	Page 5 of 5	

Distribution:

1. IT Department
2. HR
3. Related Stakeholders

CONFIDENTIALITY

This document shall be treated as confidential. No additional copies (except for copy holders) shall be made without approval of Head Department designee and a record must be kept for all the copies issued by IT Department.