IT STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh	
TITLE:	Incident Response	

SOP No.	Issue Date	Effective Date	Review Due	Copy No.	Page **1** of **5**
1.0.9					

1.0.9 Incident Response

PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to establish a framework for the identification, reporting, assessment, and resolution of IT incidents within DBL Group. This SOP aims to minimize the impact of incidents on business operations, protect sensitive information, and ensure a prompt and effective response.

SCOPE

This SOP applies to all IT systems, networks, and assets owned or operated by DBL Group.

ROLES AND RESPONSIBILITIES

Incident Response Team is responsible for restoring service to ensure business continuity.

1. Incident Categories

1.1 Security Incidents
- Unauthorized access attempts
- Malware infections
- Data breaches

1.2 System and Service Incidents
- System failures
- Network outages
- Application Errors (**IT Driven Applications, See Appendix-B**)

Incident Response Team (IRT)
- Designate an Incident Response Team (IRT) with clear roles and responsibilities.
- Establish communication channels and contact information for IRT members (**See Appendix-A**)

Incident Reporting
- All employees must report suspected incidents promptly through the designated reporting channels. IT Support contact No. Teams or Helpdesk.
- Incident reports should include details such as date, time, location, and a brief description of the incident.

SOP No.	Issue Date	Effective Date	Review Due	Copy No.	Page **2** of **5**
1.0.9					

Initial Assessment
- The IRT will conduct an initial assessment to determine the nature and severity of the incident.
- Classify incidents based on severity levels.

4. **Procedures:**

Incident Handling Procedures

Identification	• Check Device availability. • Check WAN Network and Distribution Connectivity • Use monitoring tools to identify suspicious firewall activities. • Analyze logs and alerts for anomalies.
Containment	• Isolate affected systems or segments. • Implement temporary firewall rules to block malicious traffic.
Eradication / Remove	• Remove Faulty Device with spare one or run service standalone. • Identify and remove the source of the incident. • Patch vulnerabilities or update firewall configurations.
Recovery	• Restore firewall Configuration from Backup • Restore normal operations. • Validate the effectiveness of applied measures.
Post-Incident Review	• Conduct a thorough review of the incident handling process. • Identify areas for improvement. • Update incident response plan based on lessons learned.

COMMUNICATION PLAN
- Establish internal and external communication protocols.
- Designate a spokesperson for time-to-time update to stakeholders.

DOCUMENTATION AND RECORD-KEEPING
- Maintain detailed records of all incidents, responses, and resolutions.
- Regularly update incident documentation based on feedback and lessons learned.

ABBREVIATIONS

IT STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh	
TITLE:	Incident Response	

SOP No.	Issue Date	Effective Date	Review Due	Copy No.	Page **3** of **5**
1.0.9					

SOP - Standard Operating Procedure
IT - Information Technology
IRT – Incident Response Tea

TRAINING AND CONTINIOUS IMPROVMENT

- Provide regular training sessions for employees on incident reporting procedures.
- Conduct simulated exercises to test the effectiveness of the incident response plan.

REVIEW AND REVISION

- This SOP will be reviewed annually or as needed to ensure relevance and effectiveness.

- Any updates or revisions will be communicated to all relevant stakeholders.

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.

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

Firewall security policy will be created by Information Security Team

REFERENCES

a. FDA's 21 CFR Part 11: Electronic Records; Electronic Signatures
b. GAMP 5: A Risk-Based Approach to Compliant GxP Computerized
c. Company IT Policies and Procedures
d. Industry Best Practices

IT STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh	
TITLE:	Incident Response	

SOP No.	Issue Date	Effective Date	Review Due	Copy No.	Page **4** of **5**
1.0.9					

APPENDICES

APPENDIX-A	Incident Response Team
Appendix-B	IT Driven Application List

REVISION HISTORY

REVISION DATE	REVISION NUMBER	DESCRIPTION OF REVISION
02 Feb' 24	01	First edition of the SOP

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

Distribution:
1. **IT Department**
2. **HR**
3. **Related stakeholders (Management Employee)**

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.

IT STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh	
TITLE:	Incident Response	

SOP No.	Issue Date	Effective Date	Review Due	Copy No.	Page **5** of **5**
1.0.9					